Joint Doctrine Note 2-16

Identity Activities

03 August 2016

Unclassified

PREFACE

1. Scope

The purpose of this joint doctrine note (JDN) is to provide guidance to plan, execute, and assess identity activities.

2. Purpose

A JDN is a publication that is intended to facilitate information sharing on problems and potential solutions as a supporting effort of formal joint doctrine development and revision. It provides a short term bridging solution to potential doctrine gaps. This JDN specifically addresses how identity capabilities may be coordinated and integrated to generate effects across all phases of an operation or campaign. It supplements current joint doctrine and provides context for identity activities across the range of military operations. This document was developed using current joint doctrine, extant procedures, and existing policy guidance. This JDN does not necessarily describe a position of consensus across the joint force, but it does socialize identity activities-related information and procedures in a non-authoritative document that commanders and staffs can use, as appropriate.

3. Application

The guidance in this JDN is not authoritative. If conflicts arise between the contents of this JDN and the contents of a JP, the JP will take precedence for the activities of joint forces, unless the Chairman of the Joint Chiefs of Staff provides more current and specific guidance. This JDN will, at a minimum, inform the development and revision of other JPs.

KEVIN D. SCOTT
Vice Admiral, USN
Director, Joint Force Development

Intentionally Blank

TABLE OF CONTENTS

Intentionally Blank

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

- **Presents an Overview of Identity Activities**
- **Describes Identity Activities Support to Military Operations**
- **Explains Planning and Assessment for Identity Activities**
- **Discusses Organizational Roles, Responsibilities, and Command Relationships**
- **Discusses Special Considerations for Identity Activities**

Overview of Identity Activities

Introduction

Identity activities are a collection of functions and actions that appropriately recognize and differentiate one entity from another to support decision making. They include the collection of identity attributes and physical materials; their processing and exploitation; all-source analytic efforts, production of identity intelligence (I2) and Department of Defense (DOD) law enforcement criminal intelligence products, and dissemination of those products to inform policy and strategy development, operational planning and assessment, and appropriate action at the point of encounter. These functions and actions are conducted by maneuver, intelligence, and law enforcement components.

Purpose of Identity Activities

Identity activities inform the commander by providing a greater understanding of the adversary, their capabilities and capacities, their facilitation networks and support structures, key threat personnel, and other relevant actors as well as greater situational awareness of the operational environment (OE). Identity activities provide robust, scalable, and sharable mechanisms to map and monitor the human terrain (both within the physical domains and the information environment), identify network nodes and centers of gravity, and exploit enemy vulnerabilities. Similarly, identity activities provide a rational means to assess operational effectiveness by monitoring the resilience of threat networks after an attack or maneuver.

Identify and Characterize Threat Actors and Networks. Strategic through tactical collections, conducted by maneuver, intelligence, and/or law enforcement personnel,

support the identification, characterization, and tracking of threat actors and networks to inform a comprehensive understanding and awareness of the OE and impact on the ability to successfully execute current and future missions.

Support the Planning and Execution of Operations. Commanders and staffs at all levels use identity activities, and resulting identity information, I2 and DOD law enforcement criminal intelligence products, to support planning, direction, execution, and assessment of operations. These products are crucial to commanders', staffs', and components' ability to identify and select specific threat actors/networks as targets, associate them with desired effects, and support the joint force commander's (JFC's) operational objectives.

Restrict Adversaries' Mobility and Access. Joint force vulnerability to irregular and asymmetric events and tactics is determined, in large part, by the JFC's ability to deny and degrade adversaries' mobility and access across the OE. Collected identity information and I2 analytic methodologies can be leveraged to identify threat actors and produce widely releasable products to support targeting, tactical screening, vetting, and force protection initiatives across the theater of operations. These products not only support current operations, but inform global operations, homeland defense, and national security screening and vetting activities by interagency partners.

Enhance Security and Civil Order. Identity activities provide essential information, assessments, and estimates to enhance military activities that protect personnel, facilities, and equipment; provide security for vulnerable populations, resources, critical infrastructure, and cultural properties; and support the establishment of rule of law and legitimate and stable governance structures. When required, identity activities can prove instrumental in accounting for and tracking displaced persons, aid, and resources over time and space as well as vetting individuals for positions of trust.

Assess the Effectiveness of Operations. Identity activities help to evaluate military operations by objectively assessing their impact on threat and neutral actors and networks with respect to the JFC's intent and objectives. Identity activities assist JFCs in determining if operations are producing desired or undesired effects, when objectives

have been attained, and whether unforeseen opportunities can be exploited or require a change in planned operations to respond to adversary actions.

Definitional Framework of Identity

Identity is not static. It is shaped by many inputs that, over time, are presented in varying degrees of completeness based on the context and circumstance of the collection. Identity has both fungible and immutable (even unconscious) aspects, which may be recognized, monitored, and reassessed to maintain an accurate and complete characterization of the individual entity.

In this sense, identity is the culmination of multiple aspects of an entity's characteristics, attributes, activities, reputation, knowledge, and judgments—all of which are constantly evolving. Identity is the sum of gathered descriptors and assertions and not simply a physical or current manifestation of limited attributes.

Identity Attributes

Biographic, biologic, behavioral, and reputational identity attributes form the substance and pedigree behind the analytic judgments through which privilege, access, or benefit decisions are made.

Identity Activities Operational Process

Raw identity data by itself has relatively limited utility. However, when raw identity data is collected, processed, and exploited into usable information and then fused with other information and/or intelligence, it gains greater utility in discovering unknown potential threat actors, distinguishing associations, establishing trends or patterns of life, and attributing a person or persons to specific actions or events. It requires unity of action between operational collection and all-source analysis to create actionable information.

JFC components and organizations conduct **five interrelated tasks** for the purpose of providing commanders with relevant and timely assessments and estimates to inform decisions and actions: plan and direct identity activities, collect identity information and physical materials, process and exploit collections, conduct all-source analysis, and develop and disseminate I2 and/or DOD law enforcement criminal intelligence products.

Identity Activities Support to Military Operations

Identity activities are conducted in all phases of operation, directly enable all subsequent phases, and support both the intermediate objectives of the phase as well as the strategic end state of the operation or campaign.

JFCs execute identity activities to enhance their ability to protect personnel and property; identify threats; identify personnel who are authorized access to critical infrastructure, key assets, and cultural properties; manage populations and resources; and, screen select persons for positions of trust. Identity activities enable JFCs to better understand the population and OE, protect relevant populations, and promote a partner nation's (PN's) legitimacy and influence over a population.

Intelligence Support

Intelligence means that enable identity activities are a combination of all-source analysis, collection management, reachback support, and information sharing and foreign disclosure. These means are essential aspects to identity activities.

Key considerations for intelligence support to identity activities include constant collaboration among the operations, plans, and intelligence staffs; long-term engagement with PNs; and when necessary, direct access to national intelligence centers and agencies to meet specific requirements.

Information Sharing

The effectiveness of identity activities are enhanced by access to and sharing of identity information between DOD, interagency, and multinational partners. From the onset of mission planning through the execution of complex operations, commanders and their staffs must recognize and embrace the critical requirement for routinely and continuously sharing identity information and I2 and/or DOD law enforcement criminal intelligence products across all functional domains and appropriate mission partners.

Identity Activities Planning and Assessment

Planning Imperatives

Planning should detail multiple approaches in employing identity activities as it is adapted to changing circumstances, or enable seamless transition between phases of operations. Planning should also prioritize actors

of concern; cultural sensitivities; existing international agreements to collecting, storing, and sharing personal information; and other nuances.

Joint forces need to demonstrate an understanding of the political, social, economic, and religious dynamics of the OE before executing identity activities.

Commanders must consider the geographic area, environmental elements, and the availability of power and communications equipment for forces operating in the environment. Commanders should plan for disconnected operations and determine how to mitigate challenges in collecting and matching biometric data, downloading watch lists, and utilizing document and media exploitation and forensic reachback capacities.

The unique challenges of the specific OE should be considered in order to plan the right mix of equipment and capability to mitigate these challenges, enhance effectiveness, and maintain the ability to match and share the information as quickly as possible.

In addition to the tasks defined within the identity activities operational process, commanders must consider the conditions, circumstances, and influences that affect the provision of identity activities capabilities, namely the factors that bear on the training and deployment of forces, acquisition and fielding of collection and exploitation capabilities, and the command and control of those elements across the battlespace. The availability, capacity, and effectiveness of identity activity capabilities can be severely impacted by a lack of forethought and planning related to these factors.

Assessing Identity Activities

Threat networks will adapt visibly and invisibly even as collection, analysis, and assessments are being conducted. Assessments over time that show trends are much more valuable for identity activity planning and operational support than a single snapshot over a short time frame.

Identity activities require greater application of operational art due to the complexity of the human environment of the OE. Likewise, identity activity assessments demand staffs conduct analysis more intuitively and consider both anecdotal and circumstantial information.

Identity Activities Support to Operational Assessment

Identity activity capabilities can directly support operational assessment, providing a mechanism to monitor key indicators and measure effectiveness and performance. Identity activities "hits" and various I2 products can serve as measure of effectiveness indicators of observable, measurable, system behaviors or capabilities. Task performance can be measured through various identity activity enabled events, such as the capture of a high-value target on the DOD biometrics-enabled watch list (BEWL).

Organizational Roles, Responsibilities, and Command Relationships

Whole-of-Government Effort

Exercising the full power of identity activity capabilities requires a coordinated whole-of-government effort. Since there are a number of different organizations within the US Government that contribute to identity activities, it is important to develop some level of mutual awareness of their roles and capabilities to identify potential areas for cooperation.

The Secretary of the Army is the executive agent for DOD biometrics and non-digital/multimedia forensics, which includes those disciplines relating to serology, firearms and tool marks, latent prints, questioned documents, drug chemistry, trace materials, forensic pathology, forensic anthropology, forensic toxicology, and DNA [deoxyribonucleic acid].

The Defense Intelligence Agency (DIA) Identity Intelligence Project Office (I2PO) is the defense intelligence focal point and advocate for all matters relating to I2, biometrics-enabled intelligence, and forensic-enabled intelligence. The DIA I2PO provides subject matter expertise to combatant commanders and staff on planning, executing, and assessing identity activities; I2 production; and partner engagement activities. The DIA I2PO also provides direction and oversight for DOD BEWL development, management, and sharing efforts.

The Commander, United States Special Operations Command provides direct identity activities support (e.g., training, equipment, exploitation, I2 analysis) to globally deployed special operations forces and supported geographic combatant commanders.

Multinational organizations such as **the International Criminal Police Organization and North Atlantic Treaty Organization** can also be key partners. To fully leverage these partner capabilities, commanders should seek to understand the relevant legal, political, and cultural frameworks under which they operate well before US forces are deployed to ensure all the necessary agreements, arrangements, and procedures are in place to support effective collection, processing, exploitation, data sharing, storage, and use.

With numerous stakeholders in the identity activity mission space, it is critical that unity of effort is achieved and the roles, responsibilities, and authorities of the numerous organizations are understood by the JFC.

Special Considerations

Authorities

DOD components have authority to collect, process, and exploit identity information, forensic materials, and captured materials pursuant to US and international law. These activities, however, may be subject to limitations, restrictions, or conditions on collection and data use depending on the circumstances (time, place, manner, and purposes) of the activity. JFCs and their staffs must be cognizant of these circumstances and assess their legal impacts (restrictions, limitations, or conditions), if any, on the operation and the identity activities conducted to support it.

Multinational Operations

US commanders should expect to conduct identity activities as part of a multinational force conducting military operations. These operations, which could occur in a formal multinational alliance or a less formal coalition, could span the conflict continuum and require coordination with a variety of other interorganizational partners. To effectively employ identity activities, commanders and staffs must be cognizant of differences in partners' laws, doctrine, organization, equipment, terminology, culture, politics, religion, and language, and partner to craft appropriate solutions to achieve unity of effort.

Responsible Data Sharing Requires Controls

The joint force will typically operate in a complex international environment alongside other actors that will have a need for identity information and I2 products. The sharing of identity information, while often unclassified, requires careful controls and assessment, continuously

weighing the benefits of sharing against the possible risks of data compromise and the potential for unintended use of US-provided information.

CONCLUSION

The guidance in this joint doctrine note is not authoritative.

Joint Doctrine Note (JDN) X-XX, *Identity Activities,* is a pre-doctrinal publication that presents generally agreed to fundamental guidance for joint forces conducting identity activities. Although this JDN has not been through the joint doctrine development system as described in Chairman of the Joint Chiefs of Staff Instruction 5120.02C, *Joint Doctrine Development System,* it draws on both contemporary and historical experiences to describe the documented best practices currently in use across the joint force.

CHAPTER I
OVERVIEW

"The enemy of the future will have to be found before it can be fought."

The New Rules of War,
***Foreign Policy*, March-April 2010**

1. Introduction

This publication provides guidance to the Services, combatant commanders (CCDRs), subordinate joint force commanders (JFCs), and Service component commanders to plan, execute, and assess identity activities. It also informs civilian decision makers and interorganizational partners of the fundamental principles, precepts, and philosophies that guide the planning and execution of identity activities by the Armed Forces of the United States. Identity activities are not an adjunct or ad hoc set of actions, planned and conducted separately from normal military staff functions but instead should be fully integrated into joint operational design, joint intelligence preparation of the operational environment (JIPOE), the joint planning process (JPP), operational execution, the joint targeting process, and joint assessments. The information in this publication is not intended to supersede existing joint doctrine that guides any of the existing processes, but is intended to address how a commander should integrate identity activities within these processes to enhance military operations conducted within a complex operational environment (OE).

a. Identity activities are a collection of functions and actions that appropriately recognize and differentiate one person or persona from another person or persona to support decision making. They include the collection of identity attributes and physical materials; their processing and exploitation; inform all-source analytic efforts that lead to the production of identity intelligence (I2) as well as the development of Department of Defense (DOD) law enforcement criminal intelligence products to inform policy and strategy development, operational planning and assessment, and appropriate action at the point of encounter. These functions and actions are supported by three primary functional components:

(1) **Maneuver Components.** Deployed maneuver units provide the primary collection, processing, and exploitation capabilities to support military operations. The results of these activities often provide the basis for all-source intelligence analysis supporting the production of I2 and/or DOD law enforcement criminal intelligence to meet the commander's information requirements. These products, in turn, inform, enable, and enhance continuous operational activities planned and executed to achieve the commander's military objectives.

(2) **Intelligence Elements.** Intelligence elements support identity activities. Their primary contributions to the JFC, however, are analysis and production capabilities, reachback support, and foreign disclosure. I2 is the intelligence resulting from the processing of identity attributes concerning individuals, groups, networks, or populations of interest that contributes to an assessment of an individual's potential level of threat (or trust),

capability, capacity, and intent when combined into an all-source intelligence product. Collected identity attributes provide limited value to operational commanders and tactical units without a corresponding assessment and characterization of the identity to provide relevance and context, making I2 production an essential aspect of identity activities.

(3) **Law Enforcement Components.** DOD law enforcement components support the collection, processing, and exploitation of identity attributes that enable identity activities. These components may also conduct DOD law enforcement criminal intelligence analysis and production to support investigations, identify and track criminals, assess criminal informants, and support prosecution activities. DOD law enforcement elements utilize information gathered from law enforcement sources, in a manner consistent with applicable law, to provide tactical and strategic DOD law enforcement criminal intelligence on the existence, identities, and capabilities of criminal suspects and organizations. DOD law enforcement criminal intelligence analysis is conducted under circumstances that provide a reasonable suspicion that specific individuals or organizations may be planning or engaging in criminal activity affecting DOD missions or activities.

b. Joint forces focus on planning and conducting operations, actions, and activities to favorably shape the OE, while also anticipating and preparing to execute contingency responses to crises. Establishing and characterizing the identity of persons of interest, known adversaries, and other relevant actors across time and space is an operational imperative that improves a commander's full understanding of the OE; friendly, neutral, and threat networks impacting the OE; military interaction with the local population; conduct of military operations; and the long-term domestic security of the US and its allies. Identity activities can be conducted across the range of military operations, throughout all phases of a campaign or operation, and in any level of conflict to increase the commander's awareness about the OE and enhance his ability to protect the force, persistently target the enemy across time and space, and support security and rule of law activities within a given operational area.

c. The joint force is often challenged by diverse enemies that employ both conventional and unconventional strategies. These enemies seek to avoid US strengths by employing dispersion, concealment, and intermingling with civilian populations. Concurrently, globalization and information technologies enable enemies to operate beyond traditional physical battlegrounds. The opportunities facilitated through globalization empower extremists by improving their security, mobility, and coordination allowing them affordable access to once-restricted information and technologies. Adversarial state actors, terrorists, insurgents, and transnational criminal networks, and the convergence of these networks exploit the seams and complexity of diplomatic, legal, informational, financial, and economic processes to increase their wealth, execute their agendas, and gain power and influence at the expense of regional security and US interests. As conflicts continue to become more irregular and asymmetric in nature, the need to identify, deter, deny, and degrade an adversary's mobility, anonymity, and access to the populace and enabling resources increases in significance.

d. Strategically, the US will continue to be challenged by the proliferation of weapons of mass destruction (WMD); the convergence of terrorist, insurgent, and transnational

criminal networks and affiliated groups; illicit weapons and drug smugglers; destabilizing refugee flows; and destructive cyberspace attacks. The US also faces adversaries that seek military advantage by operating within fragile states and dense urban terrain. The information and products developed through the conduct of identity activities advances the ability of maneuver, intelligence, and law enforcement elements to discover threat actors and their networks within this complex global OE; track and limit their movements; counter or diminish their capabilities and means; bar them entry to US, allied, and partner nation (PN) facilities and territories; and ultimately deter them from taking action.

e. The effective application of identity activities requires a long-term focus and the understanding that, from collection to tactical encounters, each constituent effort must be designed to support the broadest array of missions. Without this emphasis, future military operations will be undermined, degrading our ability to create desired operational effects and achieve mission objectives. Similarly, national security activities related to defeating terrorist networks, protecting our borders, and dismantling transnational criminal organizations (TCOs) will be adversely affected.

2. The Purpose of Identity Activities

Identity activities' primary purpose is to provide information on individuals and networks to inform decision making. They discover and contribute information to the all-source intelligence picture on relevant actors and networks, track their movement and help limit target mobility, and enable force protection and civil order. This purpose is supported by a range of specific roles, responsibilities, and actions that are shared, as appropriate, among maneuver, intelligence, and law enforcement organizations under the purview of, supporting, or cooperating with the JFC.

a. **Inform the Commander.** Identity activities directly support the JFC in planning, executing, and assessing the impact of operations. Identity activities inform the commander by providing a greater understanding of the adversary, their capabilities and capacities, their facilitation networks and support structures, key threat personnel, and other relevant actors as well as greater situational awareness of the OE. Identity activities provide robust, scalable, and sharable mechanisms to map and monitor the human environment (both within the physical domains and the information environment), identify network nodes and centers of gravity, and exploit enemy vulnerabilities. Similarly, identity activities provide a rational means to assess operational effectiveness by monitoring the resilience of threat networks after an attack or maneuver.

b. **Identify and Characterize Threat Actors and Networks.** Strategic through tactical collections, conducted by maneuver, intelligence, and/or law enforcement personnel, supports the identification, characterization, and tracking of threat actors and networks to inform a comprehensive understanding and awareness of the OE and impact on the ability to successfully execute current and future missions. Typically, the intelligence directorate of a joint staff (J-2) leads the identification and tracking of threat actors/networks, often with support from maneuver and law enforcement elements. Once these threat actors/networks are identified, the J-2 must continuously review them with respect to the changing situation to determine whether they remain relevant to the commander's intent and information

requirements. Throughout this process, the J-2 should exercise an understanding of the command's responsibilities; the JFC's mission and intent; the means available, including host nation (HN) and multinational forces (MNFs), interagency partners, nongovernmental organizations (NGOs), and intergovernmental organizations (IGOs); the adversary; and human environment characteristics of the operational area.

c. **Support the Planning and Execution of Operations.** Commanders and staffs at all levels use identity activities and resulting identity information, I2 products, and DOD law enforcement criminal intelligence products, to support planning, direction, execution, and assessment of operations. These products are crucial to commanders', staffs', and components' ability to identify and select specific threat actors/networks as targets, associate them with desired effects, and support the JFC's operational objectives. Due to the sensitivities of personal information, variances in social or cultural norms, and international concerns about privacy and civil liberties, the joint force will need to employ appropriate safeguards to protect identity information and I2 products from inappropriate access or use.

d. **Restrict Adversaries' Mobility and Access.** Joint force vulnerability to irregular and asymmetric events and tactics will be determined, in large part, by the JFC's ability to deny and degrade adversaries' mobility and access across the OE. Intelligence and law enforcement analysts should leverage collected identity information and all-source analytic methodologies to help identify threat actors and produce widely releasable products to support targeting, tactical screening, vetting, and force protection initiatives across the operational area. These products will not only support current operations but may inform global operations, homeland defense (HD), and national security screening and vetting activities by interagency partners.

e. **Enhance Security and Implement Civil Control.** Identity activities provide essential information, assessments, and estimates to enhance military activities that protect personnel, facilities, and equipment; control populations and resources; and protect critical infrastructure and cultural properties. When required, identity activities can prove instrumental in accounting for and tracking displaced persons, aid, and resources over time and space as well as enhancing the vetting of individuals for positions of trust.

f. **Assess the Effectiveness of Operations.** Identity activities help to evaluate military operations by objectively assessing their impact on threat and neutral actors and networks with respect to the JFC's intent and objectives. Identity activities assist JFCs in determining whether operations are creating desired or undesired effects, when objectives have been achieved, and whether unforeseen opportunities can be exploited or require a change in planned operations to respond to adversary actions. Analysis of collection and encounter information and trends, to include biometrics-enabled watch list (BEWL) encounters, and assessments of operational mission outcomes can provide insight into the effectiveness of joint operations and the resiliency of the targeted threat network or force.

3. The Global Security Environment and National Security Challenges

The strategic environment is characterized by uncertainty, complexity, and rapid change, which require persistent engagement. This environment is fluid, with continually changing

alliances, partnerships, and new national and transnational threats constantly appearing and disappearing. While it's impossible to predict precisely how challenges will emerge and what form they might take, we can expect that uncertainty, ambiguity, and surprise will dominate regional and global events. In addition to traditional conflicts that include emerging peer competitors, significant and emerging challenges continue to include irregular threats, malicious cyberspace activities, catastrophic terrorism employing WMD, and other threats to disrupt the nation's ability to project power and maintain its qualitative edge.

a. The globalization of terrorism and transnational crime, adversarial manipulation of cyberspace, rising political instability, growing ungoverned regions, and the proliferation of ethnic violence threaten US interests, and are all elements that pose an immediate risk to US security. As the security environment continues to become more complex and unpredictable, state and non-state adversaries compete for influence and access. Maintaining national security and managing inevitable changes are continuous processes that often preclude simple solutions. These challenges require well-planned and executed joint operations in conjunction with actions taken by a variety of other participants. In addition to military forces (including MNFs) and civilians, there may be a number of interagency partners, IGOs, NGOs, and elements of the private sector whose presence or influence can affect the JFC's operations.

(1) **Globalization and Cyberspace Technology.** Globalization is the reduction of barriers to transnational movement of information, ideas, money, people, goods, and services. With data processing, storage, and transmission capabilities increasing rapidly, information technology now underpins nearly all aspects of modern society. Those cyberspace technologies that enabled globalization have also enabled state and non-state actors to promote violent extremist ideology; obtain and transfer funds; recruit and train personnel; arrange transport, arms, and equipment; and sustain operational communications.

(2) **Poor Governance and Instability.** Weak and failing states and ungoverned spaces generate internal conflict and humanitarian concerns that significantly challenge regional and global security. These areas are desirable targets for adversarial state and violent non-state actors seeking to extend their power and influence.

(3) **Irregular Warfare (IW).** Adaptive adversaries, including both state and non-state actors, increasingly resort to irregular forms of warfare as effective ways to challenge conventional military powers. Advances in technology and other trends render such irregular threats more lethal, more capable of spreading widespread chaos, and considerably more difficult to counter. Multiple types of actors, from local criminals to TCOs to terrorists, to state actors employ IW tactics to further their objectives. These adversaries pursue IW strategies, employing a mix of irregular, disruptive, traditional, and catastrophic capabilities to undermine and erode the influence and will of the US and our strategic partners. Adversaries favor these indirect and asymmetric approaches because they create instability and uncertainty within the OE, thereby increasing their unrestrained freedom of action.

(a) **Terrorists.** Terrorists and terrorist organizations are characterized by the unlawful use of violence or threat of violence, which is often motivated by religious,

political, or other ideological beliefs, to instill fear and coerce governments or societies in their pursuit of goals that are usually political. Transnational political movements that use violence to advance their objectives are referred to as violent extremist organizations (VEOs) or terrorists.

(b) **Insurgents.** Typically, an insurgency begins with covert activities that steadily transition toward more overt acts of subversion, sabotage, and violence. Historically, insurgency movements were mostly characterized by nationalist aspirations and typically featured a central power base and command and control (C2) infrastructure. Modern trends are for insurgency to transcend a central power base and expand into multiple political, ideological, financial and informational areas; they also increasingly to feature a more diffuse and often not readily recognizable C2 infrastructure. This broad reach allows modern insurgency movements to attract foreign fighters, transnational terrorists, and TCOs. Effectively countering modern insurgency requires nonmilitary and nonlethal means, with the military securing critical infrastructure and the relevant population(s). Identity activities complement and reinforce many of the activities making up civil-military counterinsurgency (COIN) operations.

(c) **Criminal Networks.** Areas that lack authority or governance offer ideal conditions for the proliferation of criminal gangs, bandits, and pirates and their conduct of overt criminal behavior. Taking advantage of the breakdown of authority or the chaos of conflict, they target US or PNs' property and resources or an HN's infrastructure, cultural treasures, or natural resources. These disruptive criminal actions promote the very instability sought after by other politically, ethnically, or religiously motivated adversarial state and non-state actors. TCOs are organized international criminal associations whose primary purpose is to obtain power, influence, and monetary and/or commercial gains either wholly or in part through illegal enterprise. Since criminal networks excel at smuggling narcotics, weapons, cash, and other contraband; human trafficking; and conducting financial crimes such as counterfeiting, money laundering, and fraud, they can also provide essential logistic or other support to various other adversarial state and non-state actors.

b. Threats present in a particular operational area vary. The threat may consist of a conventional hostile military force, an unconventional militia, guerrilla forces, terrorists, criminal organizations, violent gangs, an opposing political group, a catastrophic force of nature, or a disruptive threat such as hunger or disease. The convergence of multiple threats appearing simultaneously in an OE is becoming increasingly typical. JFCs may face a host of relevant but disparate actors, each with their own grievances and objectives and each seeking varying levels of control or influence within the OE. This complexity creates the ability for adversaries to become indistinguishable from the civil population, facilitating freedom of maneuver and enhancing their ability to create disruptive effects.

c. Future OEs will likely be complex, dynamic, and unpredictable, presenting a host of new paradigms and challenges that shape the employment of joint forces across the conflict continuum. The challenges are neither new nor purely military in nature. However, today's OE requires a wide array of partners, strategies, and cross-cutting capabilities to effectively engage, disrupt, and neutralize dispersed or concealed enemies, offset their specific asymmetric advantages, and restrict their mobility and access while simultaneously securing

and stabilizing dense urban terrain and protecting civilian populations, critical infrastructure, and cultural assets. JFCs must internalize the dynamic effects these paradigms will have on each phase of operations and adequately plan to minimize their shortfalls.

(1) **Future Operations Will Continue to Be Conducted in a Multinational Environment.** US commanders should expect to conduct military operations as part of a MNF. These operations could span the conflict continuum and require coordination with a variety of United States Government (USG) departments and agencies, foreign military forces, local authorities, IGOs, and NGOs. Given the complexity of the OE, a comprehensive approach toward conducting identity activities in a multinational/inter-organizational environment increases the need for coordination and synchronization among military and nonmilitary entities. Commanders and staffs should be cognizant of differences in PN laws, doctrine, organization, equipment, terminology, culture, politics, language, and objectives, and partner to craft appropriate solutions to achieve unity of effort. With the proliferation of identity technologies and associated data resources, geographic combatant commanders (GCCs) should frequently assess multinational partners' identity capabilities. Joint and multinational exercises should ensure identity activities are synchronized and existing identity information systems are interoperable to support potential military operations.

For more information on multinational operations and interagency coordination, see Joint Publication (JP) 3-16, Multinational Operations, *and JP 3-08,* Interorganizational Coordination During Joint Operations.

(2) **Operations Will Require Whole-of-Government Contributions.** A whole-of-government approach integrates the collaborative efforts of USG departments and agencies toward a shared goal. The JFC must work with the US embassy chief of mission (COM), Department of State (DOS), and other interagency entities to integrate operations with the other instruments of national power in unified action. Establishing a whole-of-government approach to achieve unity of effort should begin during planning. Competing priorities, challenges in information sharing, and differences in lexicon can be overcome through early collaboration and coordination begun in the planning phase.

(a) **Leadership and Authorities.** Each USG department and agency has different authorities that govern the department's or agency's operation and determine its use of resources. These authorities derive from several sources: the Constitution, US law, Presidential directives, congressional mandates, and strategic direction. The longstanding nature of these authorities has created specific organizational cultures and lexicons that can profoundly affect planning and execution of identity activities by, with, and through interagency partners. Clearly defining and documenting these authorities early in planning establishes a clear understanding of identity activities' relationships. In all military operations, but most notably during military engagement, security cooperation, and deterrence, the legal authority of a department or agency to act will greatly affect the planning, approval, and execution of identity activities. JFC access to and use of identity information and I2 products will likely be affected by various interagency partners' authorities, policies, and regulations. For instance, deoxyribonucleic acid (DNA) collected by deployed Federal Bureau of Investigation (FBI) personnel in some instances may only be

later accessed and used by authorized law enforcement personnel for law enforcement purposes. Care should also be taken to ensure communication between interagency partners is clear when lexicons diverge based upon the culture and role of the organization.

(b) **Unified Action.** In the conduct of military operations, interagency partners are not a substitute for military forces. However, these partners can make military forces more capable and efficient. Just as joint interdependence is the purposeful reliance by one Service on another Service's capabilities, special operations forces (SOF) and conventional forces (CF) may rely on interagency capabilities to maximize their respective capabilities. Interagency collection, military engagement, exploitation, analysis, and dissemination capabilities may be more able or better positioned to meet the needs of the commander or support the achievement of mission objectives. The degree of interdependence will vary based on specific roles, activities, and circumstances. The JFC should seek to understand and integrate interagency identity activity capabilities and capacity into his force structure and requirements planning processes.

(3) **Balancing Near-Term and Long-Term Considerations.** Identity activities should be planned and executed to support current military operations or US diplomatic initiatives with specific consideration given to host population and foreign partner perceptions. The visibility and socio-cultural implications of certain activities or resulting outputs can have unintended strategic consequences well outside the operational area. For example, if a mass collection of biometric data is conducted to identify terrorists hiding within a village, but that information is later misused by the host government to facilitate sectarian violence, the near-term purpose might have a detrimental effect on long-term goals. The conduct of identity activities must be exercised in thoughtful, reasoned, and politically sufficient ways that both enhance US security and maintain diplomatic standing among our partners. Whenever possible, JFCs should exercise a whole-of-government approach to planning, conducting, and assessing identity activities to ensure those activities do not unduly affect national security and policy interests.

For more information on the strategic environment, refer to JP 1, Doctrine for the Armed Forces of the United States.

4. Strategic Guidance

National strategic guidance provides the foundation for the development of DOD strategy and guidance documents. Top-level strategy and general guidance for identity activities is derived from the national security strategy (NSS) and identity-specific Presidential decision directives (e.g., homeland security Presidential directives [HSPDs] and Presidential policy directives [PPDs]).

a. National Strategy

(1) **NSS.** The NSS describes the US military as a force postured globally to protect US citizens and interests, preserve regional stability, render foreign humanitarian assistance (FHA), and build the capability and capacity of our partners to assist in meeting security challenges. Vigilance is required to stop countries and non-state actors from developing or

acquiring chemical, biological, or nuclear weapons, or the materials to build them. US forces will continue to defend the homeland, conduct global counterterrorism (CT) operations, support allies, and deter aggression through forward presence and engagement. If deterrence fails, US forces will be ready to project power globally to defeat and deny aggression in multiple theaters. This strategy demands an approach that prioritizes targeted precision operations, collective action with responsible partners, and increased efforts to prevent the growth of violent extremism and radicalization that drives increased threats, including disruption of the flow of foreign fighters to and from conflict zones. Identity activities enable each of these military efforts, with outputs that provide a strong foundation from which to enhance security, as well as deter, disrupt, and dismantle violent extremists, and provide services and aid in any area of responsibility (AOR).

(2) **National Intelligence Strategy.** The National Intelligence Strategy identifies primary topics that DOD supports: cyberspace intelligence (i.e., understanding threats in cyberspace), CT, counterproliferation, and counterintelligence (CI). Additionally, the National Intelligence Strategy describes three foundational missions in support of the NSS: strategic intelligence, anticipatory intelligence, and support to current operations. Identity activities are enablers to each of these topics and missions in support of operational planning and execution as well as national security. The JFC must plan and conduct identity activities with these strategic to tactical outcomes in mind. Identity activities will help deepen the understanding of the OE to support both current operations and strategic policy and strategy development. They can enable dynamic horizon scanning to assess changing and emerging threat conditions and detect subtle shifts in trajectory that may impact operational plans and/or US national security. Finally, they will provide actionable, timely, and agile support to maintain decision advantage. Identity activities can create these effects across multiple mission areas, sometimes simultaneously, regardless of the level of warfare or phase of operation.

(3) **National Strategy for Counterterrorism.** The National Strategy for Counterterrorism is primarily focused on pressuring al-Qa‘ida’s core while emphasizing the need to build foreign partnerships and capacity and to strengthen resilience. Additionally, the strategy stresses the need for confronting al-Qa‘ida-linked threats that continue to emerge from beyond its core safe haven in South Asia. Networks of al-Qa‘ida, the Islamic State of Iraq and the Levant, and affiliated groups continue to threaten US citizens, interests, allies, and partners. The US is pursuing an approach that prioritizes targeted CT operations, collective action with responsible partners, and increased efforts to prevent the growth of violent extremism. Identity activities are key enablers for CT forces, supporting the find, fix, finish, exploit, analyze, and disseminate (F3EAD) process. The F3EAD process analyzes a terrorist organization’s nodes, capabilities, and intentions to help develop courses of action (COAs) to eliminate its capability to commit terrorist acts. Identity activities support whole-of-government efforts in this area, enabling not just SOF and conventional CT forces, but also FBI, Drug Enforcement Administration (DEA), and other law enforcement actors, and intelligence community (IC) components.

(4) **National Strategy to Combat WMD.** Adversaries of the US continue to pursue WMD to enhance their international influence and achieve greater strategic leverage against US advantages. Increased access to expertise, materials, and technologies heightens

the risk that these adversaries will seek, acquire, proliferate, and employ WMD. Countering WMD requires integrating enabling capabilities, such as identity activities, with specialized countering WMD capabilities to identify and address specific threat actors. Robust identity activities support the identification and monitoring of actors of concern; enhance analytic assessments of their capabilities, capacity, and intent; and enable both active and passive deterrents across the operational, intelligence, and law enforcement areas.

(5) **Strategy to Combat Transnational Organized Crime.** The elements of this strategy flow from a single unifying principle: the US will build, balance, and integrate the tools of American influence to combat transnational organized crime and related threats to national security and urge our foreign partners to do the same. The US recognizes transnational organized crime as a significant threat to national and international security and emphasizes US planning, priorities, and activities accordingly. For DOD, because transnational organized crime is fundamentally driven by threat actors and networks (as opposed to unit forces and weapon systems), the employment of identity activities is central to most efforts to counter transnational organized crime operations. Transnational organized crime penetration into state institutions, the crime-terrorism-insurgency nexus, illicit trafficking and smuggling, cybercrime, the critical role of facilitators, and the convergence points they share can only be effectively combated when the nodes, resources, and infrastructure (e.g., funding, logistical networks, supply chains, and safe havens) can be identified, assessed, and targeted, typically at the individual and node level. Collaboration between joint forces, the IC, law enforcement elements, interagency partners, as well as foreign partners in conducting identity activities to identify these actors/networks is a central component of this effort.

(6) **National Strategy for Homeland Security.** The National Strategy for Homeland Security seeks to guide, organize, and unify US homeland security efforts by providing a common framework with which to focus the whole-of-government on preventing and disrupting terrorist attacks; protecting the American people, critical infrastructure, and key resources; and responding to and recovering from major incidents. The strategy aims to deny terrorists and terrorist-related weapons and materials entry into our country and across all international borders and to disrupt their ability to operate within our borders. Security screening activities at national ports of entry enhances our ability to more effectively identify prospective threats. Cyberspace protection activities work to deny criminals and terrorists sanctuary in cyberspace, an inexpensive, geographically unbounded, and largely unconstrained virtual safe haven. The armed forces are crucial partners in homeland security, protecting the US from direct attacks and conducting missions to determine, deny, deter, detect, prevent, and define threats against the nation. Identity activities support this strategy by providing a cross-cutting set of mutually supportive capabilities across the operations, intelligence, and law enforcement areas. DOD identity collection, exploitation, analysis, and production activities conducted in direct support of military operations around the globe also, indirectly, support a broad variety of homeland security activities and programs at home.

b. **DOD Strategy**

(1) **Defense Strategic Guidance.** In January 2012, the Secretary of Defense (SecDef) released strategic guidance for DOD. *Sustaining US Global Leadership: Priorities for 21st Century Defense* reflects the President's strategic direction and recognizes the ten primary missions of the US Armed Forces. This guidance emphasizes the threats posed by both state and violent non-state actors. The guidance also recognizes that military forces conduct a range of activities, and states: "For the foreseeable future, the US will continue to take an active approach to countering these threats by monitoring the activities of non-state threats worldwide, working with allies and partners to establish control over ungoverned territories, and directly striking the most dangerous groups and individuals when necessary." Identity activities support a broad majority of these primary mission sets, providing a fundamental underpinning to military operations and activities seeking to achieve their stated objectives.

(2) **National Military Strategy.** Global disorder is increasingly while the comparative US military advantage has begun to erode. The US currently faces multiple, simultaneous security challenges from traditional state actors and trans-regional networks of sub-state groups. Conflict with near peer state actors employing large-scale military forces remains a possibility; however, more probable is continuing conflict with VEOs acting as pure non-state actors, or with a force composed of state and non-state actors working together toward shared objectives. Future conflicts may consist of traditional military forces assuming a non-state identity, or a VEO fielding some combined arms capability. In many locations, VEOs coexist with TCOs, further undermining stability. Because VEOs and TCOs prefer to conduct operations by, with and through the populace, while maintaining a level of anonymity by blending in, employment of identity activities to separate adversaries from civilians and assist in positively identifying threat actors and their networks increases in importance.

5. The Definitional Framework of Identity

Efforts to define identity have typically relied on the use of identity attributes (e.g., name, fingerprint images) to complete a specific identity transaction (e.g., obtaining physical access to a military base). However, reducing the operational focus of identity activities to simply collecting and exploiting specific data points demonstrates an incomplete understanding of identity. A more complete understanding of identity as a mission enabler requires a much more comprehensive assessment of identity attributes and their relationship to the individual or entity they describe (the whole being greater than the sum of its parts).

a. Identity is not static. It is shaped by many inputs that, over time, are presented in varying degrees of completeness based on the type context, capabilities, and circumstance of the collection. Identity has both fungible and immutable (even unconscious) aspects, which may be recognized, monitored, and reassessed to maintain an accurate and complete characterization of the individual entity. The required description and exactness of an individual's identity is significantly dependent on the context and circumstance of the identity transaction itself. Each transaction differs by the attributes it requires for completion and to what level of completeness and certainty those attributes must be presented.

b. The breadth of identity information, if analyzed and navigated expertly, can be used confidently to make positive identifications across time and space, identify and assess patterns and anomalies, and better anticipate the capability and intent of actors of interest. In this sense, identity is the summary (or sum total) of multiple aspects of an entity's characteristics, attributes, activities, reputation, knowledge, and judgments—all of which are constantly evolving. Identity is the sum of gathered descriptors and assertions and not simply a physical or current manifestation of limited attributes. Effective employment of identity activities requires both intelligence and operational assessments beyond just the content of identity attributes and the circumstances under which they were collected, toward a richer understanding about what the attributes themselves are describing in aggregate.

c. Identity is described by identity components that fall into one of four categories: biographical, biological, behavioral, and reputational. Figure I-1 summarizes the categories of identity attributes and their sub-elements.

(1) **Categories of Identity Attributes.** There are four main categories of identity attributes: biographical (e.g., name, address, passport number, tax records); biological (e.g., fingerprints, facial images, iris images, DNA); behavioral (e.g., cell phone records, social media, travel patterns); and reputational (e.g., statements attesting or vouching for character, criminal records, credit scores, security clearances, organizational position). Of note, however, is the fact that decisions about individuals are most routinely based on available reputation-related attributes. This creates an inextricable link between what is commonly described as "identity" and the notion of reputation. This association remains true across functional environments (e.g., financial, legal, consumer) as a driving factor to some degree in any identity transaction. Today, the ability to own property is not based fundamentally on an ability to pay the mortgage but on an ability to get a loan, which is governed significantly by the reputation established through previous financial transactions. The ability to sustain a driving privilege is determined from a reputation for obeying the law. Even the ability to successfully sell something online is impacted by the reputation built through previous sales. Thus how others identify you, is dramatically more important than how you identify yourself.

(2) **Identity Attributes.** Identity—its discovery, exploitation, characterization, and resolution—is made possible by the collection, exploitation, analysis, and management of identity attributes. Identity attributes form the substance and pedigree behind the analytic judgments through which privilege, access, or benefit decisions are made. Using the categories identified above, identity attributes can be organized into multiple sub-elements to support data collection, analysis, and management. Approximately 500 separate data types and sub-types of identity attributes that support relevant national security activities have been identified. (See Appendix D, "Identity Attributes and Sub-Elements," for more information on identity attributes.) While this list is certain to evolve based on user preference, mission, and authority, it provides a useful framework to support collection planning, exploitation efforts, analysis, as well as I2 and DOD law enforcement criminal intelligence product development. The sub-elements in Figure I-1 generally describe identity attributes that will be relevant to achieving objectives across the conflict continuum:

Categories of Identity Attributes

Categories of Identity Attributes			
Biographic	**Biologic**	**Behavorial**	**Reputational**
Nonphysical information related to an individual	Measurable and observable physical characteristics of an individual	A range of actions and mannerisms characterizing an individual's behavior	What an individual or organization knows or says about another individual
Identity Attribute Sub-Elements			
• Core personal • Addresses • Employment • Educational • Military Service • Family • Cohabitants • Aliases	• Individual static • Physical attributes (hair/eye color) • Scars, marks, tattoos • Familial • Group • Fingerprints, iris, face, palm print, voice, and DNA [deoxyribonucleic acid]	• Financial transactions • Law enforcement records • Digital personas • Social affiliations • Commercial transactions • Media consumption / production • Body language (gait, posture, eye movements, hand gestures, typing patterns) • Micro-expressions (brief involuntary facial expressions)	• Judicial judgements • Sworn statements • Public licenses • Financial (historical) • Community observations • Employer evaluations

Figure I-1. Categories of Identity Attributes

(a) **Biographical.** Biographic attributes describe attestable facts about an individual's life.

(b) **Biological.** Biologic attributes contain the measurable and observable physical characteristics of an individual.

(c) **Behavioral.** Behavioral attributes refer to the array of physical actions and observable emotions associated with an individual. Behavioral attributes span a range of actions and mannerisms characterizing an individual's conduct and demeanors in reaction to their environment. They reflect an individual's internal or external, conscious or subconscious, overt or covert, voluntary or involuntary responses. Some behavior changes with age, learning, or experience, while some specific traits such as personality and temperament may be consistent. Past behavior is used in predictive behavioral modeling to estimate the probability of future behavior. On the individual level, this analysis identifies recurring patterns of behavior to inform decision making.

(d) **Reputational.** This category contains information about how an individual is objectively or subjectively seen or judged by a third party based on investigation or experience. The categories of identity attributes and their sub-elements are presented in Figure I-1.

See Appendix D, "Identity Attributes and Sub-Elements," for more information.

6. Identity Activities Operational Process

Identity activities are of greatest value when they contribute to the commander's decision-making process by providing reasoned insight into threat actors, their networks, and the conditions that affect their behavior. Raw identity data by itself has relatively limited utility. However, when raw identity data is collected, processed, and exploited into usable information and then fused with other information and/or intelligence, it gains greater utility in discovering unknown potential threat actors, distinguishing associations, establishing trends or patterns of life, and associating a person or persons with specific actions or events. The process that drives identity activities is built on the fundamental requirement to inform the commander's decision cycle. It requires unity of action between operational collection and all-source analysis to create actionable information. This operational cycle is depicted in Figure I-2.

a. Identity activities offer the commander a variety of assessments and estimates and inform other intelligence products that facilitate understanding of the OE. Identity activities also help in discovery and persistent targeting of threat actors across time and space, increased force protection postures, JFC support to HN rule of law and proper governance, and populace and resource control measures. Assessments and estimates, focused on the individual identity, can be situationally applicable to the local current operation or current operations in a separate AOR, future operations, and/or intelligence or law enforcement activities. For example, biometric identification of a local insurgent actor in Afghanistan today can inform subsequent SOF operations in Africa, counternarcotic activities in Latin America, and/or homeland security screening at US ports of entry if the insurgent is encountered again in the future. With accurate and relevant I2 and/or DOD law enforcement criminal intelligence estimates, commanders gain an advantage in the OE by understanding an enemy's or adversary's network, intent, and capabilities, potentially enabling the targeting and interdiction of enemy operations. Regardless of the situation, I2 assessments and estimates enable commanders to formulate plans and make better decisions based on this knowledge.

b. Identity activities provide the basis for common terminology and procedures. Joint force components and organizations conduct five interrelated steps for the purpose of providing commanders with relevant and timely assessments and estimates to inform decisions and actions. The five tasks are: plan and direct identity activities; collect identity information and physical materials; process and exploit collections; conduct all-source intelligence and/or DOD law enforcement criminal intelligence analysis; and develop and disseminate I2 and/or DOD law enforcement criminal intelligence products. These steps integrate the roles of the planner, operator, technical and threat analyst, and commander into a single recursive process to ensure robust support to military operations regardless of

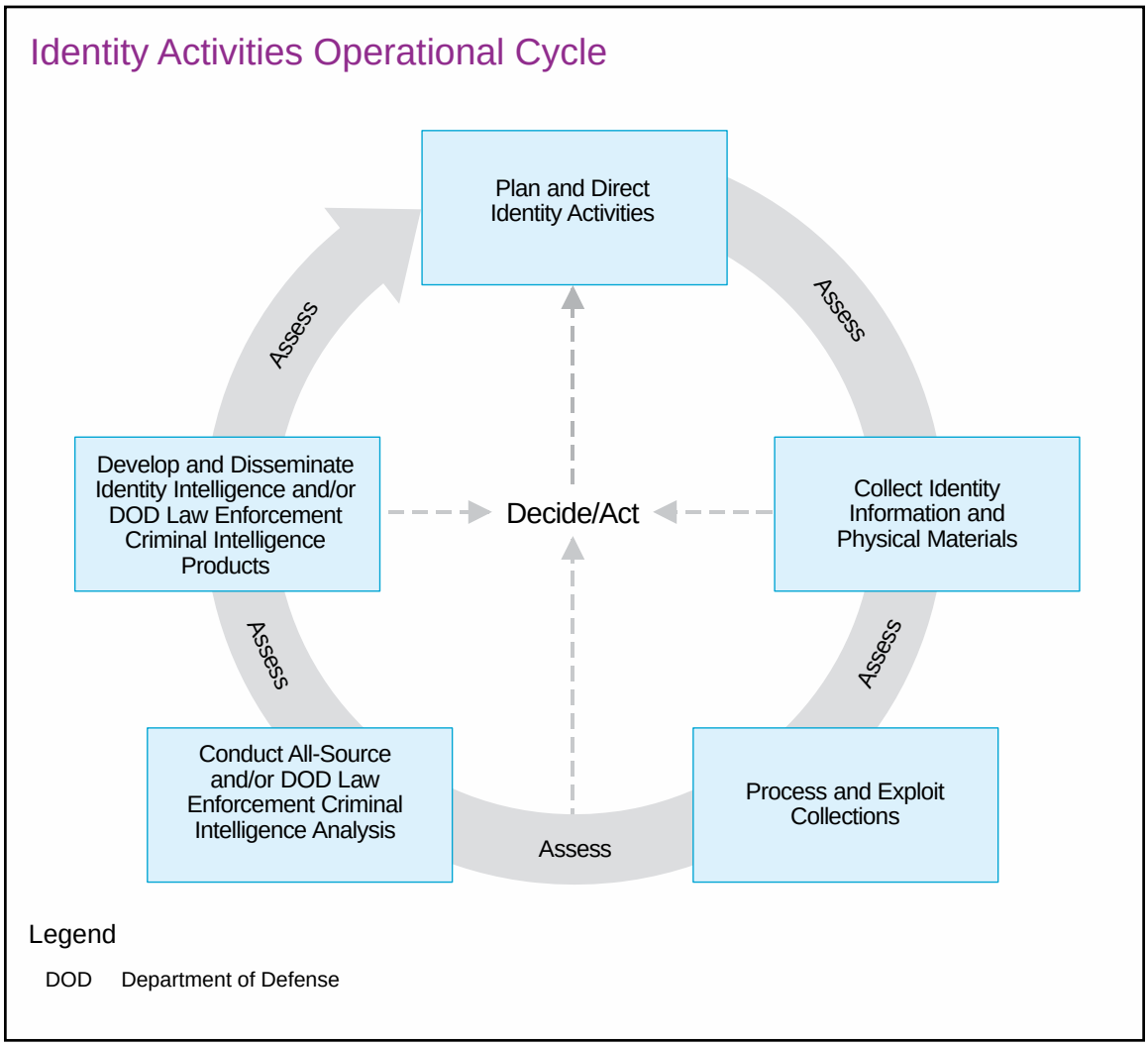

Figure I-2. Identity Activities Operational Cycle

operational phase or level of warfare. The process is nonlinear, and each step can result in actionable information to inform the commander's decision-making process, as well as future planning. The tasks within the identity activities operational process are conducted continuously as part of tactical operations executed across the OE.

(1) **Plan and Direct Identity Activities.** Planning and direction functions include, but are not limited to: the identification and prioritization of identity-related information collection requirements; the development of a concept of operations (CONOPS) and architectures required to support the commander's mission; tasking subordinate maneuver, intelligence, and/or law enforcement elements for the collection of identity information or the production of I2 and/or DOD law enforcement criminal intelligence products; submitting requests for additional collection, exploitation, or analytic capabilities to higher headquarters; and submitting requests for collection, exploitation, or all-source production support to external supporting entities (e.g., PNs, HN, interagency elements). Identity activities planning and direction occurs continuously as part of the command's adaptive planning effort. Support to crisis action planning allows for the prioritization of identity

activity capabilities across all ongoing operations and simultaneous planning efforts and products, such as JIPOE. Conversely, support to deliberate planning informs the development and prioritization of capacity and enhances readiness to respond to potential crises. Through these efforts, planners determine the personnel, equipment, and information sharing and intelligence architecture essential for identity activity support to joint operations.

(2) **Collect Identity Information and Physical Materials.** Collection includes those activities related to the acquisition of identity attributes (i.e., biographical, biological, behavioral, and reputational data), forensic materials, and documents and electronic media of operational interest. Collection is conducted by CF, SOF, and DOD law enforcement agencies. While some identity information (e.g., attributes contained on an identity credential) can be used immediately at the point of collection, most collected data and materials are sent to authoritative data repositories or local, regional, or reachback facilities or laboratories for appropriate processing and exploitation. Planners should ensure theater communication architectures are enabled to efficiently move data and materials to meet operational response requirements. Collection managers continuously monitor the results, not only of data and material collection but also processing and exploitation. Collection managers continuously assess the effectiveness of the identity attribute and material collections in meeting the JFC's requirements as part of the command's evaluation and assessment processes.

(3) **Process and Exploit Collections.** During processing and exploitation, raw collected identity data and physical materials can be examined and analyzed by automated systems and/or specialized personnel to determine their information value, correlate data to previously collected data, and report findings to command and analysts trained in I2 production. Processing and exploitation includes data normalization, correlation across identity attributes (e.g., biometric matching and name based matching), forensic analysis, technical (i.e., electronic and mechanical) analysis, and document and media translation and content analysis as well as reporting the results of these actions to appropriate intelligence and/or DOD law enforcement production elements. Processing and exploitation may be federated or performed by the same element that collected the data. Commanders should organize their theater and reachback exploitation asset responsibilities to facilitate efficiency and ensure unity of effort.

(4) **Conduct All-Source and/or DOD Law Enforcement Criminal Intelligence Analysis.** I2 is the intelligence product resulting from the processing and all-source intelligence analysis of identity attributes concerning individuals, groups, networks, or populations of interest. DOD law enforcement criminal intelligence is the result of the collection, analysis, and interpretation of all available information concerning known and potential criminal threats and vulnerabilities of supported organizations. Identity attributes (i.e., biographical, biological, behavioral, and reputational information related to individuals) and other information and intelligence associated with those attributes gathered from all intelligence disciplines or law enforcement sources are integrated to produce I2 or DOD law enforcement criminal intelligence, as appropriate. I2 utilizes enabling intelligence analysis activities, like biometrics-enabled intelligence (BEI), forensic-enabled intelligence (FEI), and document and media exploitation (DOMEX) to contribute to the discovery of the existence of unknown potential threat actors; associate individual actors to other persons, places,

events, or materials; analyze patterns of life; and characterize their level of potential threats to US interests. This analysis leverages codified analytic methodologies and compliance with the Office of the Director of National Intelligence (ODNI) intelligence analysis standards to produce timely and actionable estimates and assessments to inform the commander's decision cycle. DOD law enforcement criminal intelligence utilizes information gathered from law enforcement sources, in a manner consistent with applicable law, to provide tactical and strategic DOD law enforcement criminal intelligence on the existence, identities, and capabilities of criminal suspects and organizations. DOD law enforcement criminal intelligence analysis is conducted when there is a reasonable suspicion that specific individuals or organizations with a connection to DOD may be planning or engaging in criminal activity.

(5) **Develop and Disseminate I2 and/or DOD Law Enforcement Criminal Intelligence Products.** I2 and DOD law enforcement criminal intelligence products can be presented in many forms. They may be oral presentations, hard copy publications, or electronic media. The means are determined by the needs of the user and the implications and criticality of the intelligence. Rather than being the end of a process, I2 and/or DOD law enforcement criminal intelligence production is a continuous dialogue between the user and the producer. I2 production for joint operations is accomplished by units and organizations at every echelon. However, reachback elements like joint intelligence centers, Service intelligence centers, and combatant command (CCMD)-assigned intelligence brigades typically form the backbone of any operational I2 production support. DOD law enforcement criminal intelligence products are created by DOD law enforcement agencies as prescribed by the JFC.

See Appendix B, "Identity Intelligence Specialized Products," for more information.

(6) **Conduct Operational Assessments.** Commanders and their staffs conduct assessments of identity activities to determine whether they are creating the desired effects. Identity activities require a greater application of operational art due to the complexity of the human environment of the OE. Likewise, identity activity assessments demand staffs conduct analysis more intuitively and consider both anecdotal and circumstantial information. Assessments over time that show trends are much more valuable for identity activity planning and operational support than a single snap shot over a short time frame. Tactical unit reporting such as patrol debriefs and unit after-action reports may provide the most valuable information on assessing the impact of identity activities, particularly when correlated across an OE.

c. Identity data, forensic insights, and translated document and media content combined with other information and intelligence through all-source analytic assessments provide the operational commander with actionable information to support operational planning and tactical action. The identity activities operational process is organized to directly inform the decision cycle at all echelons.

Intentionally Blank

CHAPTER II
IDENTITY ACTIVITIES SUPPORT TO MILITARY OPERATIONS

"Modern threats challenge us to think carefully about our future missions. Complex operating areas, especially in the urban littorals, demand the ability to understand the human terrain [environment]. Increasingly, our enemies will use anonymity as cover; while widespread coverage of military operations will demand minimization of collateral effects from our operations. Both of these can limit freedom of action. While identity [human component of the operational activities] will never remove the fog of war entirely, they give the Joint Force the tools necessary to operate with greater precision in engagement, maneuver, and fires."

Brigadier General Michael S. Groen,
Director of Intelligence,
US Marine Corps, 2014

1. General

a. Traditionally, identity activities have mainly been used to enhance physical security. Today, identity activities are also used to enable safe and effective operations by providing essential information on the enemy, relevant actors, networks, and populations to inform operation planning, execution, and assessment throughout each phase of an operation or campaign. Identity activities provides a correlating mechanism to associate and link identity information to other collected information to create an extensive knowledge base of the enemy, adversary, friendly, and neutral variables that characterize the OE. This knowledge base increases the overall understanding of the physical, cultural, and social environment in which the joint force operates and helps to create desired effects across the OE. The exploitation of this body of information enables decision makers to better influence the OE, which in turn enhances the ability to control the population, influence key actors, and diminish the enemy's freedom of maneuver to achieve their operational objectives.

b. Identity activities are not a new phenomenon within joint operations. JFCs have been employing identity activities since before the Vietnam conflict using the limited capabilities at their disposal. The prevalence and value of identity activities in today's operations are a function of the exponential increase in technology that has fundamentally changed the way identity information is collected, processed, exploited, and disseminated. These technologies continue to proliferate and often bridge cultural, geographic, and language barriers. Many technologies enable identity activities to be adaptable in a scalable and tailorable approach to support regionally focused missions, bilateral and multilateral military exercises, and security cooperation activities.

c. At the strategic level, identity activities are dependent on effective CCMD execution, interagency and PN sharing, collaboration, and decentralized multidimensional approaches. Strategic partnerships and military engagements yield information and intelligence, thereby informing analytic efforts, producing I2 and/or DOD law enforcement criminal intelligence products, and providing actionable decision support to JFCs and other national security components worldwide. JFCs and their staff must have a thorough understanding of the legal, policy, and architectural frameworks to effectively conduct identity activities across

the range of military operations. Identity activity requirements should be strategically applied throughout staff planning processes in a synchronized and integrated manner. Joint, interagency, and multinational sharing arrangements and Service-level agreements should be arranged during pre-mission or contingency planning and strategic and operational-level lessons must be studied and integrated.

d. At the operational level, identity activities utilize collaborative and decentralized approaches that blend technical capabilities and analytic tradecraft to identify and characterize individuals within the operational area. Specialized collection tools and exploitation processes, combined with all-source intelligence analysis of the collected data, allow commanders to better understand the human environment of the OE. Operational-level echelons employ identity activities and capabilities to support many of their core mission sets. They employ them throughout the OE in support of military operations. JFCs must coordinate and synchronize identity activities at the operational level to ensure friendly plans and operations are complementary. For example, in Afghanistan, the initial organization of deployed forensic exploitation assets created redundancy and inefficiency between counter-improvised explosive device (C-IED)-focused labs and other deployed assets. Only once formal joint force staff structures were put in place and operational control of the resources realigned, was the full efficacy of the capability demonstrated through significantly increased operational effectiveness.

e. At the tactical level, the primary focus of identity activities is identifying persons of interest and determining their disposition at the point of encounter; connecting them to places, people, events, and materials of interest; enhancing force protection measures; enhancing and substantiating targeting activities; and vetting individuals for positions of trust. Effective use of these activities helps to restrict adversary mobility, identify threats, monitor or track persons of interest, and manage detainees and displaced persons. Identity activities help to counter espionage, sabotage, subversion, insurgency, terrorism, and crime. They enable civil control; separation of warring factions; HN rule of law activities; evaluation of persons for amnesty, reintegration, and reconciliation programs; investigation of crimes against humanity; and transition to civil authority. Identity activities help to shape the OE, deter threat actors and networks, reestablish safe and secure environments, provide humanitarian relief, and develop or strengthen the legitimacy of HNs, while protecting the force, enhancing cybersecurity, and reinforcing HD efforts.

f. Identity activities support many joint functions across the conflict continuum, including protection, fires, and movement and maneuver. The broad nature of identity activities requires several key factors to underpin the operational art and operational design of operation planning. The ways in which identity activities are conducted is often just as important as access to the adequate means to conduct them. JFCs can choose multiple operational approaches to employ identity activities throughout each phase of an operation to achieve military objectives. Each approach has advantages and drawbacks but all may be restricted in their implementation if adequate pre-mission planning does not occur.

2. Identity Activities Throughout the Phases of Operations

Identity activities are conducted in all phases of an operation, directly enable all subsequent phases, and support both the intermediate objectives of the phase as well as the strategic end state of the operation or campaign. The transition of identity activities between phases is primarily a function of refocusing efforts toward the evolving goals and objectives of the commander. The main challenge for planners is to adeptly plan for timely deployment and fielding of identity activity capabilities by correctly anticipating the capacity requirements for long-lead time and/or low density collection, exploitation, and analysis elements within the event-driven phasing of operations. The following is an explanation of identity operations throughout a notional five phase operation.

a. **Phase 0 (Shape) and Phase I (Deter).** In these phases, the command focuses on building the identity activity capacity of both US forces and MNFs and demonstrating to PNs the value of sharing identity data and other related information to include biometrics, forensics, and document and media collections.

(1) During phase 0, identity activities enable or enhance normal and routine force protection measures. Establishing identity activities is a central element in civil security missions, while deterring potential adversary access to relevant populations, resources, and critical infrastructure. Identity activities may also be used to enhance proper governance by supporting the rule of law, facilitating fair and open elections, enabling positive identification at points of entry, distinguishing between warring factions, and protecting vulnerable groups. Identity activities must be integrated across DOD and HN forces to ensure unity of effort and promote operational legitimacy. This may require building or enhancing partner capabilities and capacity. Theater campaign plans (TCPs) should provide guidance to coordinate phase 0 identity activities and share identity information.

(2) Many actions in phase I build upon the security cooperation activities from phase 0. Civilian or military law enforcement and CI personnel are employed to investigate adversary actions. These forces exploit identity databases during investigations to identify disruptive and destructive persons. By seeking out sites once occupied by adversaries, mission-tailored forces collect relevant information identifying persons of interest, establish associations, and attribute nefarious actions to appropriate persons or groups. By exposing adversary actions, identity activities can deter additional undesirable action, while setting the conditions for intervention.

(3) TCPs in conjunction with integrated country strategies and COM country plans, identify and work with specific partners within each AOR to build identity activity relationships as a part of security cooperation. Military engagements, in addition to bi-lateral exchanges by interagency partners coordinated and de-conflicted at the interagency level by the National Security Council (NSC), provide DOD with access to identity information and capability that can support current and future operations.

(4) Building partnerships and partner capacity early, prior to phases II or III, shortens the time needed to reach full operating capability and the required collection tipping

point (described in Chapter III, "Planning and Assessment") during major combat or contingency operations.

b. **Phase II (Seize the Initiative) and Phase III (Dominate).** During these phases, when the situation permits, JFCs will conduct identity activities to support lethal operations, intelligence and CI activities, detainee management, populace and resource control, stabilization activities, and force protection. Building upon actions conducted during phases 0 and I, previously accumulated identity information will enhance intelligence production, facilitating target development and follow-on planning. Populace and resource control measures enabled by identity activities support the JFC's efforts to restrict adversary mobility and access, augment CI operations to identify destructive and disruptive elements, and enable better management of detainees, displaced persons, and refugees. Biometric identification of enemy prisoners of war (EPWs), refugees, displaced persons, and civilian internees not only allows for better control of detained personnel, but also facilitates the later identification of people who may become adversaries. Furthermore, this same information can be used to support criminal or war crime prosecutions. Conducting identity activities to identify and exploit Internet and social media use by adversaries is a critical enabler to the JFC's planning, warning, information operations (IO), and communication synchronization activities.

c. **Phase IV (Stabilize).** This phase is typically characterized by the transition from sustained combat operations to stability operations. The purpose of the stabilize phase is to reestablish a safe and secure environment; provide essential government services, emergency infrastructure reconstruction, and humanitarian relief; and restore local political, economic, and infrastructure stability. Identity activities within this phase include controlling access to the local population, resources, and critical infrastructure and vetting select indigenous persons for their assumption of sensitive duties or positions of trust. Identity activities are essential enablers in the stabilize phase, directly supporting a shift to presence, security force assistance (SFA), reconciliation, institution building, and rule of law activities and provide essential government services and humanitarian relief. Identity activities directly support phase IV operations; strengthen security components, such as national police and criminal courts, to help legitimize the HN government; and help set the conditions for a political settlement. Throughout phase IV operations, CF and SOF may work alongside HN authorities to execute the planning and direction, collection, processing and exploitation, all-source analysis, and I2 production and dissemination steps of the identity activities operational process. Doing so brings increased levels of confidence to HN forces, adds legitimacy to US activities, and ultimately supports a successful transition of identity activity capabilities to the HN government. However, CF and SOF should expect to provide significant supporting capabilities to facilitate and sustain this transition over the long-term. The joint force may also be required to integrate the identity activities of other supporting interorganizational partners until legitimate HN entities are functioning.

d. **Phase V (Enable Civil Authority).** Phase V aims to help civil authorities regain their ability to govern, administer services, and address other needs of the population. Identity activities in this phase may be at the behest of HN civil authorities or they may be under their direction depending upon the level of HN state capacity. They support the civil authority's efforts to provide essential services to the indigenous population, namely security

and support to rule of law. Employment of identity activities may require the involvement of interagency partners and may be a supporting element to activities led by other USG departments and agencies.

3. Identity Activities Support Across the Range of Military Operations

Military operations vary in scope, purpose, and conflict intensity across a range that extends from military engagement, security cooperation, and deterrence activities to crisis response and limited contingency operations and, if necessary, to major operations and campaigns. Identity activities can be conducted across the range of military operations at all levels of warfare, and throughout all phases of a campaign or operation. The JFC must integrate and synchronize identity activities within and across missions and functions (offense and defense) within each phase of any operation.

a. JFCs use identity activities in a wide variety of combat and noncombat situations as part of a cohesive operational strategy to support the TCP. Identity activities support scalable, distributed operations performed by CF, SOF, or supporting interagency elements with adequate training and standardized equipment. Identity activities may take place across the conflict continuum from building PN capacity, deterring local or regional threat actors/networks, and enabling crisis response operations or limited contingencies to countering terrorist incidents and supporting major operations and campaigns that protect or advance national security interests.

b. Across the range of military operations JFCs execute identity activities to enhance their ability to protect personnel and property; identify threats; identify personnel who are authorized access to critical infrastructure, key assets, and cultural properties; manage populations and resources; and, screen select persons for positions of trust. Identity activities enable JFCs to better understand the population and OE, protect relevant populations, and promote a PN's legitimacy and influence over a population. These activities enhance scalable sustainable approaches to preventing, deterring, disrupting, or defeating irregular threats and are an important component in denying irregular threats the resources, cover and concealment, and maneuver offered by local populations.

(1) **Military Engagement, Security Cooperation, and Deterrence Activities.** Military engagement, security cooperation, and deterrence are ongoing specialized activities that establish, shape, maintain, and refine relations with other nations and domestic civil authorities at all levels of conflict. The primary purpose of these activities, which may include identity activities, is to enable the GCC to build indigenous capabilities that deter threat actors and networks and shape the OE to a desired set of conditions that facilitate stability and future operations. Shaping activities include development of PN and friendly military capabilities and capacity, identity information exchange and I2 and/or DOD law enforcement criminal intelligence sharing, interagency coordination, and other efforts to ensure access to and stability of critical regions around the globe.

(a) Identity activities as a part of military engagement include noncombat activities conducted by DOD components (e.g., headquarters staff, Naval Criminal Investigative Service, SOF). GCCs conduct routine military engagements to build trust and

confidence, share information, coordinate mutual activities, maintain influence, build defense relationships, and develop allied and friendly military capabilities for self-defense and multinational operations. DOD components conduct military engagement with nations' military or civilian security forces and authorities. Activities might include establishing supportive partnership agreements on conducting identity activities. During military engagement, the US and its partners may establish supportive partnership agreements on conducting identity activities or handling identity information between US forces and the PNs' armed forces.

(b) Security cooperation is DOD interactions with foreign defense establishments to build defense relationships that promote specific US security interests, develop allied and friendly military capabilities for self-defense and multinational operations, and provide US forces with peacetime and contingency access to an HN.

(c) Deterrence reduces threat actor/network activity by presenting a credible threat of identification, tracking, and specific counteraction that would deny the success of an organization's use of terrorism, criminal enterprise, and/or guerilla tactics or degrade its legitimacy or influence over a population. Deterrence of an adversary who uses terrorism, illicit means, or asymmetric methods to achieve its objectives is a difficult task. Identity activities aid deterrence by delivering relevant identity information on key persons and their associations to a certain time, place, activity, or event to the JFC. This information can be used to deter or deny key individuals' mobility or access to resources. Identity activities increase the possibility of early detection of planned, attempted, actual, or suspected hostile acts and improve the probability that threat operations will fail and their perpetrators captured. Military engagement and security cooperation activities can deter future adversarial activity by presenting a credible threat that US and regional partner identity activities would reveal threat actors to security or law enforcement entities, endanger their personnel or resources, or render their organization ineffective. Deterrence in one region may force threat actors to temporarily move to another, which may deter or disrupt the organization's activities for a period of time.

(2) **Crisis Response and Limited Contingency Operations**

(a) **Crisis Response.** The President and SecDef can respond to imminent threats or actual acts of terrorism by executing Chairman of the Joint Chiefs of Staff (CJCS) or GCC's crisis response plans. Crisis response operations are rapid, relatively small-scale, of limited duration, and may involve multiple threat locations. Identity activities can provide immediate enhancement to force protection activities, persistent targeting of known threat actors, and support a variety of offensive, defensive, or stabilization functions.

(b) **Limited Contingency Operations.** Identity activities during limited contingencies may include identification of insurgent, terrorist, or criminal actors and efforts to gain insights into threat and facilitation networks that pose an imminent threat to a US mission abroad. After threat actors and their organizations are located, US forces may use I2 products to inform and enable strikes or raids to neutralize or reduce the threats as well as other operations as directed by SecDef or GCC.

(3) **Major Operations and Campaigns.** The JFC may conduct identity activities in support of all phases of operations to support the disruption of adversarial state and non-state actors' use of asymmetric tactics and enable a more comprehensive understanding of the OE. Identity activities can restrict enemy and adversary mobility and access across and beyond the assigned operational area, identify key personnel, enable monitoring or tracking of persons of interest, and enhance the vetting of individuals for positions of trust. Identity activities in support of major operations and campaigns should be sustained, synchronized, and integrated across multiple operational areas, and designed to support both current operations and potential follow-on operational phases.

c. **Additional Military Activities and Operations.** Joint doctrine characterizes the employment of US military forces by types of activities and operations in order to describe the nature of the effort, tasks, tactics, and other aspects to inform future operations, training, and professional education. There are four broad categories under which identity activities can be conducted: security cooperation, overseas military operations, HD, and cyberspace operations (CO).

(1) **Security Cooperation.** Security cooperation activities are all US military efforts to improve other nations' ability to provide security and services for its citizens, govern, prevent terrorist and criminal actors from using the nation's territory as a safe haven, and promote long-term regional stability. They include:

(a) **Security Sector Assistance (SSA).** SSA refers to a group of programs by which the US provides defense articles, military training, and other defense-related services to foreign nations by grant, loan, credit, or cash sales. SSA equips, trains, and develops capabilities and capacities in foreign military and security forces. A GCC's TCP may include activities to provide identity activity-related security assistance to a nation's military and, when authorized, civilian security forces, and may be combined with similar security assistance to neighboring countries to develop regional identity activity capabilities to address cross-border threats and act in a coordinated effort. SSA related to identity activities must be well coordinated with interagency partners to ensure unity of effort and synchronization in our military engagements with PNs.

(b) **Foreign Internal Defense (FID).** FID programs encompass the diplomatic, economic, informational, and military support provided to another nation to assist its fight against subversion, lawlessness, insurgency, terrorism, and other threats to security. US military support to FID focuses on operational assistance to HN personnel and collaborative planning with interorganizational and HN authorities to anticipate, preclude, and counter threats. FID supports HN internal defense and development programs. US FID programs may use identity activities to help a nation defeat an organized movement attempting to overthrow its lawful government or address other threats to the internal stability of an HN, such as civil disorder, illicit drug trafficking, and terrorism.

For more information, see JP 3-22, Foreign Internal Defense.

(c) **FHA.** FHA consists of DOD activities, normally in support of the US Agency for International Development within DOS, conducted outside of the US and its

territories to directly relieve or reduce human suffering, disease, hunger, or privation. The assistance provided supplements or complements the efforts of the HN civil authorities or agencies that may have the primary responsibility for providing humanitarian assistance. Identity activity capabilities can greatly enhance DOD's operational reach in providing rapid and robust response capabilities by supporting population management, distribution of services, management of resources, and identification and tracking of threats (e.g., criminals, human traffickers, drug traffickers).

For more information, see JP 3-29, Foreign Humanitarian Assistance.

(d) **SFA.** SFA consists of DOD activities that contribute to unified action by the USG to support the development of the capacity and capability of foreign security forces and their supporting institutions. Foreign security forces consist of civilian and military organizations, to include law enforcement, border security, intelligence, SOF, and CF. SFA may provide identity activity training and equipment to foreign security forces; access to DOD processing and exploitation capabilities; and sharing of relevant identity information, I2, and DOD law enforcement criminal intelligence. Supported by appropriate policy and legal frameworks, building capacity and capability is a long-term continuing process, in which all actors contribute to enhancing the HN's human, technological, organizational, institutional, and resource capabilities. These capabilities and associated results must be self-sustaining for the HN. Designing capacity and capability building initiatives for identity activities requires an understanding of what identity management processes the HN has in place and the sustainability requirements for any new or additional capabilities introduced. All identity activity initiatives must consider the potential for misuse; the political, social, and cultural sensitivities of the targeted population; and the perceptions of external actors. The primary role of identity activities in SFA is to develop identity activity capabilities and capacity within the HN's security forces. However, joint forces may also have a role to support efforts led by other USG departments and agencies to enhance the partner's identity activity abilities supporting broader elements of governance, economic development, essential services, rule of law, and other critical government functions.

(2) **Overseas Military Operations**

(a) **Offense, Defense, and Stability Operations**

1. **Offensive and Defensive Operations.** Combat operations vary widely depending on the context of the operation and the objective. In striving to achieve military strategic objectives quickly and at the least cost, JFCs will normally seek the earliest opportunity to conduct decisive offensive operations. Nevertheless, during sustained offensive operations, select elements of the joint force may need to pause, defend, resupply, or reconstitute, while other forces continue the attack. Strong area security and force protection initiatives (e.g., security vetting, threat identification, warnings) require a comprehensive understanding of the human environment. The JFC may need to continuously execute identity activities to help protect personnel and property and secure the local population, critical infrastructure, cultural assets, and other strategic resources. Identity activities inhibit access of enemy infiltrators, spies, saboteurs, subversives, and assassins

across the OE and impede their freedom of movement during offensive and defensive operations.

2. **Stability.** These initiatives set the conditions for interaction with multinational partners, competitors, adversary leaders, military forces, and relevant populations by developing and presenting information and conducting activities that affect their perceptions, will, behavior, and capabilities. The JFC will likely conduct stability operations in coordination with interorganizational partners and the private sector in support of HN authorities. Identity activities can be used to support a broad spectrum of stability activities; from conducting strikes and raids on terrorist or insurgent organizations to helping to secure the population and vetting local nationals nominated for sensitive positions or training within HN institutions. Identity activities, comprising both civil and military applications, facilitate an efficient transition toward civil authority.

See JP 3-07, Stability, *for more information.*

(b) **Countering Threat Networks (CTN).** CTN is the aggregation of activities across the USG that identifies and neutralizes, disrupts, or destroys designated threat networks. CTN operations primarily seek to counter terrorist, insurgent and criminal networks. Identity activities in support of CTN operations entails exploiting and analyzing collected identity attributes; producing and disseminating I2 products to positively identify persons of interest; linking them to other actors, activities, events, locations, and networks; and, if applicable, placing them on DOD watch lists (e.g., DOD BEWL). At the strategic level, identity activities are dependent on interagency and PN information and intelligence sharing, collaboration, and decentralized approaches to gain identity information and intelligence, provide analyses, and vet the status (friendly, adversary, neutral, or unknown) of individuals outside the JFC's operational area who could have an impact on the JFC's missions and objectives. Interagency partners and PNs also rely on the JFC for identity data developed at the tactical level to facilitate strategic-level decision making and actions. At the operational level, identity activities employ collaborative and decentralized approaches that blend technical solutions and analytic capabilities to provide identification and vetting of individuals within the operational area and enhance awareness and understanding of the OE. At the tactical level, identity activities provide the commander an effective tactical capability that is tailorable and responsive to enhance force protection and support targeting activities. Collection and analysis of identity-related data helps tactical commanders further understand the OE and decide on the appropriate COAs with regards to individual(s) operating within it.

See JP 3-25, Countering Threat Networks, *for more information.*

(c) **COIN.** Effectively employing identity activities as a COIN tool can be labor and time intensive. Identity capabilities may be employed to restrict the insurgents' and insurgent supporters' area of influence and protect vulnerable populace, critical infrastructure, essential resources, and cultural property. Aptly transitioning identity activities to HN security forces may strengthen fragile governance, instill legitimacy, and undermine insurgent influence. Developing identity information and I2 products on key insurgent personnel enables accurate targeting to degrade or destroy the insurgent center of

gravity. Since insurgents are considered unlawful combatants by the HN, identity information also enables their detention and prosecution.

See JP 3-24, Counterinsurgency Operations, *for more information.*

(d) **Peace Operations (PO).** The diplomatic, informational, economic, and military efforts to return a nation to stability and legitimate governance may be spoiled by the actions of terrorist, insurgent, or criminal actors. The JFC should assess the requirement for identity activities during PO. The fundamental requirement for impartiality within PO requires the JFC to act on behalf of the peace process and not show preference for any faction or group over another. Impartiality does not apply to possible spoilers such as terrorists. The JFC, within the command and operational framework of the specific PO, should determine whether actors hostile to the peace process use violent or unlawful tactics and design identity activities in coordination with USG departments and agencies, HN, and PNs.

See JP 3-07.3, Peace Operations, *for more information.*

(e) **Counterdrug Operations.** Counterdrug activities are provided by DOD to support foreign military forces and law enforcement agencies to detect, monitor, and counter the production and distribution of illegal drugs. DOD policy recognizes that illicit drug traffickers and terrorists often use the same methods and that in many cases, traffickers and terrorists are one and the same. Insurgents can also use illicit drug production or trade to fund their operations. JFCs can effectively execute identity activities to identify, track, and enable the interdiction of these threat actors/networks.

See JP 3-07.4, Counterdrug Operations, *for more information.*

(f) **Noncombatant Evacuation Operations (NEOs).** NEOs are conducted to assist DOS in evacuating US citizens, DOD civilian personnel, and designated HN and third-country nationals whose lives are in danger from locations in a foreign nation to an appropriate safe haven due to crisis events. The JFC may use identity activities to support the combat identification of personnel to be extracted as well as to manage evacuated individuals once at the relocation site. Identity activities can also be used to identify or contribute to the identification of threat actors among the evacuated population.

See JP 3-68, Noncombatant Evacuation Operations, *for more information.*

(g) **Countering WMD.** The intersection of states, state-sponsored terrorism, non-state terrorists, and WMD proliferation represents one of the greatest security challenges facing the US. JFCs must develop and maintain a comprehensive understanding of both the actors and materials that affect the OE. To accomplish this, the JFC needs to locate, identify, characterize, assess, and predict threats against US and partner interests. Attribution is a task that provides dissuasion and deterrence value if properly signaled to actors of concern but can also be valuable during response activities. Identity activities support an in-depth understanding of threat actors that may employ WMD and the potential effect of a WMD release on the OE. In addition to other F3EAD capabilities, a JFC may use identity activities to enhance and enable the ability to systematically locate, characterize, disrupt, neutralize, or

destroy WMD threat networks before they can move, transfer, or employ WMD as well enable attribution of WMD-related events to threat actors and networks.

See JP 3-40, Countering Weapons of Mass Destruction, *for more information.*

(h) **Unconventional Warfare (UW).** Identity activities are a principal nonlethal capability used by the JFC to support all phases of UW. One of the JFC's primary challenges is to identify the key actors within the resistance forces, the hostile government or occupying power, and relevant populations to inform UW planning and execution activities. To do this effectively, the JFC must collect identity attributes, correlate and weave them into an identity, understand how that identity relates to others in the OE, and understand the threat or opportunity they represent for achieving the desired objectives. Identity activities follow a continuous and iterative process, as JFCs must frequently reassess these judgments throughout each phase of UW and use identity information and products to enable other fundamental components of UW support (e.g., CI, training, and logistics). These activities support not only the selection and enabling of resistance members but also the intelligence support to resistance activities and operations.

See JP 3-05.1, Unconventional Warfare, *for more information.*

(3) **HD.** Identity activities as a part of HD represent a global effort that crosses AOR boundaries and requires an integrated and synchronized effort among interagency and multinational partners for mission accomplishment. Identity activities contribute to HD by enabling and enhancing the protection of US residents through active layered identification, characterization, and tracking of threat actors. DOD identity activities play an essential role in HD by collecting, assessing, and operationalizing usable identity information on threat actors worldwide. This information enhances the ability of consular officers, federal law enforcement agents, IC personnel, and state and local elements to provide a defense-in-depth against individual threat actors seeking to do harm within the boundaries of the US.

See JP 3-27, Homeland Defense, *for more information.*

(4) **CO.** The JFC faces a unique set of challenges while executing CO. Cyberspace presents the JFC with many threats ranging from nation states to individual actors who actively seek to mask their identities and/or their actions. Connecting a cyberspace actor (cyber-persona) or action to an actual individual, group, or state actor with sufficient confidence and verifiability to hold them accountable is perhaps the most challenging aspect of defeating threats in cyberspace CO. One individual may have multiple cyber-personas, which may vary in the degree to which they are factually accurate. Conversely, a single cyber-persona can have multiple users. In cyberspace it is also possible to "spoof" or assume the identity of some other entity (human or nonhuman). Consequently, attributing responsibility and targeting in cyberspace is difficult. Because cyber-personas can be complex, with elements in many virtual locations but normally not linked to a single physical location or form, significant intelligence collection capabilities and I2 production efforts are required for the joint force to gain sufficient insight into and situational awareness of a cyber-persona to enable effective targeting and creation of desired effects. The effective

employment of specialized identity activities are vital to the development of actionable identification and attribution of threat actors operating in cyberspace.

See Appendix A, "Identity Activities Support to Operational Missions," and JP 3-12, Cyberspace Operations, for more information.

4. Identity Activities in Operational Art and Operational Design

a. In conducting joint operation planning, commanders and their staff apply operational art and operational design using JPP. The interaction of operational art and operational design for the integration of identity activities into operation planning provides a bridge between strategy and tactics, linking national strategic aims to tactical combat and noncombat operational use of identity information that must be executed to accomplish these aims.

b. To effectively integrate identity activities into JPP, the JFC and staff must understand what the capabilities entail and how to use them to optimal advantage. Identity activities must be pervasive throughout all staff planning processes and elements within JPP. They must be embedded within the operational design of all unit operations.

c. The greatest potential benefit of a focused identity activities operational design effort is the seamless integration of identity activity capabilities within the JFC's explicit efforts to solve particularly ill-defined problems. Operational design is essential in building a common perspective or common operational picture and shared understanding to create unity of effort. During operational design efforts, including a focus on individuals who have been linked to enemy locations, events, materials, and networks provides the commander a greater degree of understanding about the complexities of the OE. The commanders' and staffs' understanding of the OE, in turn, enables them to further visualize and integrate identity activities and capabilities into the mission.

d. This relationship between the application of identity activities within operational art, operational design, and JPP continues throughout execution of the campaign or operation. A continual assessment of the commander's plans and execution allows redirection of the various identity activity approaches, as appropriate.

See JP 5-0, Joint Planning, *for more information.*

5. Intelligence Support

a. Intelligence is a principle enabler of identity activities. Intelligence support to identity activities is primarily reflected in the intelligence organizations, capabilities, and processes that are involved in the collection, processing, exploitation, analysis, and dissemination of I2, the intelligence resulting from the processing of identity attributes concerning individuals, groups, networks, or populations of interest. Collected identity attributes are of limited value to operational commanders and tactical units without a corresponding assessment and characterization of the identity developed through fused all-source analysis and production. These assessments require access to both local information sources and national systems to fully meet the intelligence needs of the commander. CF and

SOF often deploy with limited intelligence personnel and equipment. Direct augmentation from reachback components and external intelligence organizations will often be necessary to meet evolving requirements.

b. Key considerations for intelligence support to identity activities include constant collaboration among the operations, plans, and intelligence staffs; long-term coordination with PNs; and when necessary, direct access to national intelligence centers and agencies to meet specific requirements. JFC intelligence staffs collaborate with the combat support agencies (CSAs), United States Special Operations Command (USSOCOM), interagency partners, and the IC to build a fused intelligence picture. Distributed identity activities conducted under IW conditions over a large operational area may require an operations-intelligence fusion capability at the applicable tactical level to ensure that actionable intelligence, which may be perishable, is available to operational commanders in a timely manner.

c. Intelligence support to operations begins with the articulation of mission requirements. This includes identification of information and production requirements to support targeting and the priority intelligence requirements (PIRs) for the commander's decision cycle. For identity activities, commanders should ensure that any requirement for intelligence support to identity activities is identified.

(1) **I2.** I2 is the intelligence resulting from the processing and all-source analysis of identity attributes concerning individuals, groups, networks, or populations of interest. I2 reflects an all-source analytical effort that fuses numerous identity attributes (i.e., biological, biographical, behavioral, and reputational information related to individuals) and other information and intelligence associated with those attributes or individuals of interest. I2 utilizes enabling intelligence activities, like BEI, FEI, and DOMEX to discern potential threat actors by connecting individuals to other persons, places, events, or materials; analyzing patterns of life; and characterizing their level of potential threats to US interests. These assessments can be used to characterize the OE; identify adversary strategies and COAs; and provide insight into the physical, cultural, and social environments that influence human behavior. JFCs can exploit biometric, forensic, document and media data collections and integrate that data with other all-source intelligence to locate and track unattributed identities across multiple or disparate encounters, cases, and events, and map out human networks. Collections are processed through the appropriate DOD and interagency databases, exploited to produce intelligence, and then disseminated to deployed forces and throughout the USG. I2 products enable real-time decisions in any phase of operation.

(2) **Collection Management.** Collection management is the process of converting intelligence-related information requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required. Collection will occur over the course of both military engagement, security cooperation, and deterrence activities and military operations. The joint intelligence operations center (JIOC) executes collection management authority on behalf of a joint force J-2 and exercises collection requirements management for certain assets and all national resources. Through coordination with the operations directorate of a joint staff (J-3) via fragmentary orders and operation orders, the JIOC delegates or identifies

collection management authorities for identity activities for subordinate components and joint task forces (JTFs). Collection managers must know of the capabilities, limitations, survivability, and lead times of available identity activity collection systems, as well as the processing and exploitation, analysis, and production timelines to complete and disseminate an I2 or DOD law enforcement criminal intelligence product. Collection managers must also be able to coordinate the employment of all available collection capabilities. This includes requesting external theater and national level resources to acquire needed information.

(a) Joint intelligence organizations are directly responsible for providing the CCMD and subordinate joint force with a common, coordinated intelligence picture by fusing national and theater intelligence, law enforcement, and CI information into all-source assessments and estimates. Joint intelligence activities focus on determining the joint force's intelligence needs based on the mission and commander's guidance; prioritizing intelligence requirements; developing an optimal collection plan and strategy; identifying collection or production shortfalls that may require resource augmentation, intelligence federation, or direct national-level analytic/collection support; and then evaluating satisfaction of needs and requirements and adjusting intelligence services and support accordingly.

(b) The JIOC is the focal point for the CCMD's intelligence planning, collection management, analysis, and production effort, and is organized in a manner best suited to satisfy the CCDR's intelligence requirements. The CCMD JIOC maintains visibility on all intelligence collection resources available to the command, aids the CCDR and staff in determining intelligence gaps and shortfalls in intelligence collection capability, and recommends solutions to mitigate them. The JIOC also seeks to ensure timely support by submitting requests to IC production centers through the national agency representatives in direct support to the command.

(c) Since most identity activity collection will likely be executed by non-intelligence units, the JIOC will need to integrate and coordinate its collection planning with non-intelligence CF and DOD law enforcement components, such as the Naval Criminal Investigative Service and Army Provost Marshall, and relevant interagency components to ensure the broadest level of collection assets are employed to meet the commander's identity information needs. For biometric information, the Defense Intelligence Agency (DIA) Identity Intelligence Project Office (I2PO) supports the collection planning efforts of the GCCs and USSOCOM, facilitates interagency coordination of collection activities, and enables military engagement activities seeking collection of or access to foreign partner identity data. Additionally, identity attributes that are collected through military engagements with foreign partners are monitored through an NSC foreign partner engagement strategy and governance process. CCMDs who conduct identity data collections through military engagement activities should include them within the TCP and inform the relevant Under Secretary of Defense for Policy (USD[P]) country desk officers of any identity activity-related military engagement planning efforts at the earliest opportunity. Depending on the method of military engagement (e.g., SSA), DOS approval of the activity may also be required.

(d) Commanders should also ensure they have sufficient capacity to transport collected data and materials to processing and exploitation elements located within the

operational area or as reachback capabilities within the continental US. Effective triage protocols should be present to ensure exploitation capacity is not overwhelmed.

(3) **Reachback Support**

(a) Combat operations limit, to varying degrees, the amount and types of forward-located intelligence support provided. As such, identity activities typically benefit from an assigned reachback effort. Reachback capabilities allow forward-deployed forces to leverage national and Service assets outside the operational area for classified and open-source research, data, and capability to provide actionable intelligence. Sufficient communications bandwidth and connectivity are essential to reachback support.

(b) Interagency partners can provide valuable reachback support. For example, the FBI's Terrorist Explosive Device Analytical Center (TEDAC) provides national-level exploitation support for improvised explosive devices (IEDs), allowing deployed expeditionary exploitation capabilities to maintain their focus on the commander's time-sensitive requirements. Similarly, the National Media Exploitation Center (NMEC) provides timely and strategic content analysis of captured documents and digital media. This analysis directly supports theater DOMEX exploitation capabilities to meet operational requirements. Processing and exploitation reachback can also be coordinated through multinational partners who possess similar capabilities.

(4) **Intelligence Sharing**

(a) Intelligence sharing is accomplished at all levels and during many operations; the requirement expands with proximity to the operational forces. Therefore, it is imperative that the JFC and J-2 understand the limits and restrictions on information sharing. To facilitate sharing with PNs and HNs, I2 and DOD law enforcement criminal intelligence products should be written for release whenever possible. Given the support many of these intelligence products provide to force protection and targeting activities, even products whose classification has been downgraded to unclassified//for official use only to enable broad operational use, may be sensitive and should not be shared with PNs and HN unless authorized through foreign disclosure review prior to release.

(b) The foreign disclosure officer (FDO) of the CCMD is key in any intelligence-sharing plan with interagency, intergovernmental, nongovernmental, or multinational partners. The FDO is versed in the National Disclosure Policy (NDP) and can guide the JFC and staff in the proper procedures for the release of classified or sensitive information. The FDO provides staff review and advises the JFC on approval of sanitized or downgraded I2 products. In the absence of an on-site FDO, I2 products that require sanitization or downgrading for release to third parties should be referred to the producing agency through the command representative from that agency or may be coordinated through the request for information (RFI) process. Since this process may be time-consuming, the JTF/J-2 should request deployed FDO support to optimize timely intelligence sharing requirements.

(c) The FDO uses NDP and the Director of National Intelligence (DNI) guidance to promulgate directives to CCMD intelligence analytical elements on sanitization processes and procedures, including tear line reporting. Tear line reports are derived from US intelligence products and written in such a way as to readily and quickly provide essential operational information without revealing the information's source. Tear line reporting is a mechanism for analytical elements at the CCMD, JTF/J-2, and component levels to provide intelligence-derived I2 products to partners (PNs without established intelligence sharing agreements; state, local, and tribal elements; and intergovernmental and nongovernmental entities). CCDRs are delegated authority to conduct tear line reporting, which can be further delegated in writing to the JTF commander and below. The J-2 should use the principle of "write to release" when deciding whether to produce a tear line. That is, the information should be provided to the interagency, intergovernmental, nongovernmental, or multinational partners if it is determined that the information contained in the report is relevant to the partner's mission and can be released to the partner.

d. **Theater Intelligence Operations.** Intelligence operations are carried out by designated and trained personnel to support requirements and activities within the intelligence process. Intelligence operations that affect, use, or support identity activities include, but are not limited to, human intelligence (HUMINT), CI, and signals intelligence (SIGINT).

6. Sharing of Identity Information, Identity Intelligence, and Department of Defense Law Enforcement Criminal Intelligence

a. The effectiveness of identity activities can be enhanced by access to and sharing of identity information among DOD, interagency, and multinational partners. Within this context, sharing consists of the transfer of identity information, I2, or DOD law enforcement criminal intelligence products, from one organization or system to another. The sharing of identity information and I2 and/or DOD law enforcement criminal intelligence products has proven essential to mission success in recent operations. DOD policy states that identity information and materials collected during the course of military operations and activities will be considered DOD data and that that data must be collected, stored, and managed according to approved technical standards; appropriately secured and handled in accordance with published security classification guidance; and shared and/or made available to appropriate mission partners to the maximum extent allowed by US law and DOD policy. From the onset of mission planning through the execution of complex operations, commanders and their staffs must recognize and embrace the critical requirement for routinely and continuously sharing identity information and I2 products and/or DOD law enforcement criminal intelligence products across all areas and appropriate mission partners. Accordingly, commanders at all levels should determine and provide guidance on what information and products need to be shared with whom and when.

b. The amount of identity information or I2 and/or DOD law enforcement criminal intelligence products required to be shared varies widely based on the nature of the military operation. In general, combat operations with MNFs require much more robust information and intelligence sharing than humanitarian or peacekeeping operations. The JFC must scale

the organization's capability to share identity information, I2, and DOD law enforcement criminal intelligence products, accordingly.

c. Information sharing activities should ultimately be designed to enhance the identity activities capability enterprise. The strength and effectiveness of identity activities are closely linked to the size and completeness of its accessible framework of authoritative data sets. The utility of identity activities is greatly reduced if new data is not promptly integrated with existing data sets, which must be routinely and continuously enhanced through direct enrollments, encounters, and collections; robust interagency partnerships; aligned allied programs; and military engagements. When initiating operations in a new theater, collections are more likely to be matched against existing interagency and/or allied data sets than existing DOD holdings. Collected materials are more readily exploited, sourced, and attributed if there is an appropriately sized library of samples available for comparison. New threats can be identified, even before boots are on the ground, if strong data sharing partnerships are formed and actively nurtured with priority countries. Regardless of the mechanism, dynamic information sharing activities are the cornerstone to ensuring that authoritative data sets contain the breadth and depth of information needed to support operational activities in any AOR around the globe.

d. To support identity information sharing activities, DOD has established a comprehensive policy and technical framework to sustain identity activities. This framework encompasses data transmission mechanisms; military engagement schemas; data management policies to facilitate information discovery, accessibility, and use; and designated support organizations to enable and sustain identity activity information sharing from the strategic to the tactical levels.

(1) **Data and Material Transport Mechanisms.** The USG maintains multiple authoritative repositories of identity, forensic, and DOMEX information. These repositories act as strategic assets and capabilities supporting a variety of national security missions and activities across the operations, intelligence, and law enforcement areas. For identity activities to be successful, collected data and materials have to move from the point of collection to these authoritative repositories for processing, comparison, and analysis. There are multiple methods for this movement to occur:

(a) **Web-Based Portal.** DOD maintains web-based portals for transmitting identity data and digitized forensic materials to appropriate entities for processing, comparison, and analysis. These portals are available on both the Nonsecure Internet Protocol Router Network and the SECRET Internet Protocol Router Network (SIPRNET), and in some instances, on the North Atlantic Treaty Organization's (NATO's) Battlefield Information Collection and Exploitation System (BICES). When required, the portals can be accessed through an operation-specific Combined Enterprise Regional Information Exchange System capability. The portals are broadly accessible through multiple communication links, including in some instances, the indigenous communications infrastructure. However, bandwidth issues can be a significantly limiting factor, especially in hostile or uncertain OEs. Planners should ensure the geographic CCMD communications system directorate of a joint staff (J-6) has granted the authority to operate one or both of these portals on the theater-

based network and the appropriate service-level agreements have been executed with each of the authoritative repository management organizations.

(b) **Dedicated Server Architecture.** A few primary collection systems within the DOD arsenal operate entirely off of their system-specific infrastructure of servers. These servers operate in a distributed fashion from a central hub, ensuring warehoused data is continuously synchronized with minimal latency. The central hub provides the connection to DOD's authoritative repositories which, in turn, manage automated and semiautomated information exchanges with interagency and other partner repositories. These systems can provide robust support in confined theaters with a well-developed communications network. However, they can require significant manpower to maintain and service.

(c) **Dedicated Air Transport.** To support certain missions, commanders may choose to dedicate specific air assets to collecting and transporting accumulated data and materials to designated theater installations. Dedicated air is typically used when timeliness is the critical factor for mission success (i.e., C-IED). However, planners should anticipate potential increases in latency and gaps in the delivery schedule when those air assets are temporarily re-tasked to support higher priority efforts.

(2) **DOD Identity Repositories.** DOD maintains several key information systems that organize and maintain collected, processed, exploited, and analyzed information and materials to support subsequent identity activities, analysis, and operations:

(a) **DOD Automated Biometric Identification System (ABIS).** The DOD ABIS is the authoritative database for biometric information collected on non-DOD personnel throughout the course of military operations. The DOD ABIS contains fingerprints, iris scans, facial images, and palm prints collected through direct enrollments, site exploitation activities, direct allied and multinational submissions, and information shared by interagency and foreign partners. This data is normalized and stored in an unclassified repository for comparison against future biometric collections.

(b) **National DNA Index System (NDIS) and Joint Federal Agencies Intelligence DNA Database (JFAIDD).** Both NDIS and JFAIDD store and manage digitized DNA profiles. DOD employs the NDIS Combined DNA Index System software within its instantiation. NDIS is limited to DNA profiles collected during the course of law enforcement activities. DNA profiles loaded into NDIS are automatically checked against other DNA index systems connected to the national architecture to support investigations. NDIS data must be collected and used for law enforcement purposes and can only be accessed by law enforcement professionals. JFAIDD was created as the interagency intelligence counterpart to the NDIS.

(c) **Biometric Identity Intelligence Resource (BI2R).** BI2R is an analytic tool set, data repository, and production support system that ingests biometrics and associated intelligence data on biometrically enrolled persons of interest. BI2R disambiguates identity data from multiple systems and networks and pushes correlated data to other intelligence systems to baseline and resolve encountered identities. The system automatically estimates and scores the threat probability for each identity maintained within

the system and prioritizes production workflow based on those scores. BI2R is the primary mechanism used to develop and maintain the DOD BEWL.

(d) **Harmony.** Harmony is the centralized repository for foreign military, technical, and open-source documents and digital media of operational and intelligence value and their translations for the intelligence, national law enforcement, defense, and homeland security communities. Harmony is accessible through multiple secure networks (e.g., SIPRNET, Joint Worldwide Intelligence Communication System, Stone Ghost, BICES) and provides a flexible, modular, field deployable collection tool suite.

(e) **Detainee Reporting System (DRS).** The DRS is the mandated detainee accountability database for all DOD components. It creates official biometrically linked detainee records for DOD and the USG. The web-based system allows for real-time data sharing with deployed systems, and is an essential tool for detainee operations that is used to issue Geneva Convention required internment serial numbers, and to collect and submit biometric and biographical information, including medical and property files, on all detainees.

(3) **Authoritative Interagency Repositories.** In addition to DOD data sources, JFCs can leverage authoritative interagency repositories to support identity activities across the conflict continuum:

(a) **FBI's Next Generation Identification (NGI).** NGI is a national law enforcement biometric and criminal history system maintained by the FBI's Criminal Justice Information Services Division. NGI provides automated fingerprint, iris, palm, and face search capabilities; latent matching capabilities; electronic image storage; and electronic exchange of biometrics files to more than 18,000 law enforcement agencies and other authorized interagency partners. NGI is the largest criminal fingerprint database in the world, housing the fingerprints and criminal histories of more than 70 million subjects.

(b) **Department of Homeland Security (DHS) Automated Biometric Identification System (IDENT).** IDENT is the central DHS-wide system for the storage and processing of biometric and associated biographical information for national security; law enforcement; immigration and border management; intelligence; background investigations for national security positions and certain positions of public trust; and associated testing, training, management reporting, planning and analysis, or other administrative uses. IDENT stores and processes biometric data—digital fingerprints and facial images—and links biometrics with biographical information to establish and verify identities presented at the point of encounter. IDENT maintains more than 140 million biometric files of individuals seeking entry to the US.

(c) **DHS TECS.** TECS (not an acronym) is the updated and modified version of the former Treasury Enforcement Communications System. TECS is DHS's primary border security and enforcement system that's managed by US Customs and Border Protection (CBP). It supports the sharing of information about people who are inadmissible or may pose a threat to the US. TECS provided the ability to create and query "lookout

records." It helps CBP officers determine the admissibility of more than 900,000 visitors annually and approximately 465,000 vehicles daily.

(d) **Terrorist Identities Datamart Environment (TIDE).** TIDE is the USG's central repository of information on international terrorist identities. Maintained by the National Counterterrorism Center (NCTC), TIDE serves as the USG's central and shared knowledge bank on known or suspected terrorists (KSTs) and international terrorist groups, supporting various terrorist screening systems (e.g., watch lists) and the IC's overall CT mission. The TIDE database includes, to the extent permitted by law, all information the USG possesses related to the identities of individuals known or appropriately suspected to be or to have been involved in activities constituting, in preparation for, in aid of, or related to terrorism (with the exception of purely domestic terrorism information). TIDE information is accessible to authorized users via a secure network interface.

(4) **Military Engagement.** CCDRs also increase DOD's accessible data holdings through military engagements. These activities facilitate and strengthen data sharing relationships to broaden USG access to identity information on actors, networks, and population sets of operational interest that are out of the direct reach of US forces. Each CCMD has established an office to manage the employment of identity activities within the GCC's AOR. These offices, in coordination with the Joint Staff (JS) J-5 (Strategic Plans and Policy), DIA I2PO, and the appropriate USD(P) country desk officers plan and execute military engagements to gain access to and collect foreign partner data on actors of interest.

(a) To support the CCDR's military engagement efforts, the Office of the Secretary of Defense (OSD) has approved a template to facilitate the negotiation of formal identity data sharing arrangements with foreign partners. These arrangements are planned and negotiated by the GCC, endorsed by the appropriate COM, and approved and executed by the appropriate assistant secretary of defense within the Office of the Under Secretary of Defense for Policy (OUSD[P]). GCCs may seek to develop memorandums of cooperation (MOCs) with PNs to share information, ensure technical interoperability and operational congruence during future multinational operations, and/or to support independent PN activities that support GCC objectives. The resulting nonbinding MOC provides a long-term mechanism with which to guide mutually supportive collection efforts, support distributed counter threat network activities, align US and PN interests, and increase regional security all while increasing the size and quality of the authoritative reference data sets applicable to various CCMD missions and theaters.

(b) CCDRs follow an ordered military engagement process that begins with including targeted military engagements within the CCMD TCPs and the relevant integrated country strategies. Identity activity military engagements can range from simple bilateral data sharing arrangements to security cooperation (e.g., train and equip) activities that involve multiple interagency partners and/or NSC approval. Regardless of the desired outcome, GCCs must work through the JS J-5 country officer to inform and coordinate with the USD(P) country desk as early as possible in the planning stages. This will help to ensure CCMD identity activity engagements support DOD and national foreign policy objectives and do not run afoul of the NSC foreign partner engagement governance framework. Each military engagement proposal must also be reviewed for legal sufficiency by the CCMD

legal counsel and, if appropriate, the DOD Office of General Counsel for International Affairs. PN identity activity security cooperation and data sharing activities must comply with both US and HN laws and regulations. In addition to DOD reviews and approvals, GCCs must engage the appropriate US embassy country team(s) to gain COM approval for the proposed military engagement. The CCMD entry point for the embassy country team is the senior defense official (SDO)/defense attaché (DATT), who should have situational awareness of all identity activities being planned or executed by, with, through, or within the target country. GCCs should request a foreign partner viability assessment from the country team to inform military engagement planning once the initial concept proposal is complete. COM approval should not be sought until the country team has completed this assessment. GCCs may execute identity activity military engagements upon the concurrence of the USD(P) and the approval of the COM.

(c) To facilitate integration and synchronization of USG prioritization, engagement, and sharing activities, the NSC has established an international engagement governance framework for identity information. The implementation plan provides a whole-of-government approach to leverage USG department and agency engagement activities to build strategic partnerships with PNs and increase the mutual national security benefit of these activities. It establishes a coordination mechanism to ensure foreign partner engagements are integrated, synchronized, and deconflicted, as appropriate, and executed in accordance with defined national security objectives. In accordance with this plan, CCDRs, through the USD(P), shall provide the national security community sufficient visibility into their military engagement activities to ensure each effort serves the broadest range of USG interests, avoids the inadvertent loss of capability and/or confusion by PNs, prevents duplication of effort, and fully considers any foreign policy objective-based issues and reservations.

(d) Standardization impacts DOD's ability to share identity information with foreign partners at all levels of warfare. To avoid the negative operational effects and costs associated with translating and reformatting identity data, GCCs are encouraged to address the receipt and processing of identity data for each nation within their AOR in their TCPs. Additionally, CCDRs must consider the interoperability of chain-of-custody standards, systems, and data both between their foreign partners and with the US. Properly addressing these considerations and identity data quality will enable all partners to utilize identity information to support their military objectives. While each PN retains ultimate authority for data sharing agreements consistent with its legal framework, TCPs can establish sharing recommendations, facilitate forums for developing these agreements, and suggest solutions that minimize partners' standards and systems differences.

(5) **Data Management Policies.** Effective data sharing requires robust data management techniques and procedures. While authoritative repository data stewards will handle the bulk of these efforts, the CCDR retains important responsibilities.

(a) Quality collections are primarily affected by the significance the JFC places on training and routine quality assurance assessments. It is incumbent on operational commanders to stress the status of identity information and material collections as a professional military endeavor to his subordinate commanders, staff, and rank and file

personnel and to communicate his expectation of high quality collections appropriately. Commanders should ensure collection activities are included within unit training schedules and predeployment training programs. In-theater support (e.g., technical representatives, field support engineers) should also be leveraged to provide additional unit spot training as needed.

(b) DOD policy requires all biometrics systems to conform to approved standards and specifications. The DOD standard for biometric data is the Electronic Biometric Transmission Specification. Forensic collection and exploitation standards generally mirror law enforcement protocols and procedures, although some are operation-specific and outcome-specific in their implementation (e.g., some forensic exploitation conducted to inform intelligence targeting is not required to meet evidentiary standards). Strict adherence to approved standards has a direct positive effect on database quality and processing speed and accuracy. Conversely, loose adherence can create long-lasting data and material processing and management issues and cause adverse ripple effects throughout the enterprise. Commanders at all levels should enforce the common and complete application of approved standards in all identity collections and activities.

(c) Data collected through CCMD military engagement activities must be thoroughly reviewed, assessed for veracity, and validated prior to submission to the appropriate authoritative data source for processing and exploitation. While DOD considers all identity information to have operational value, CCDRs must anticipate the myriad downstream DOD and interagency customers that may use that information to support their own national security missions and activities. Reasonable efforts must be made to ensure erroneous or fraudulent information is not ingested into DOD repositories. Furthermore, if fraud or PN misuse of DOD capabilities is detected, GCCs must immediately inform the appropriate country team(s) and responsible DOD officials (e.g., Defense Forensics and Biometrics Agency [DFBA], DIA I2PO, USD[P]).

(d) To facilitate effective data management within the authoritative DOD and interagency repositories, CCDRs must ensure information and materials received from a PN are appropriately tagged prior to submission for processing and exploitation. Tagging should comply with the specifications defined by the appropriate authoritative data stewards and remain consistent across all information and materials provided by the PN.

(e) As part of the formal information sharing arrangement, PNs may request responses/feedback (e.g., match reports, forensic reports, I2 products) for the information, intelligence, and/or materials they submit to DOD for processing/exploitation and analysis. Prior to releasing information back to the PN, JFCs must conduct a foreign disclosure review to ensure provided information will not enable misuse or objectionable conduct by the receiving entity. Foreign disclosure reviews must take place for all identity activity information and products regardless of content security classification. When possible, JFCs, in coordination with the DIA I2PO and USD(P), can define common response content and formats that can automatically be released to submitting partners for unclassified information (e.g., red, green, amber responses; limited match reports; tear line alert text). Release of classified information must conform to ODNI partner or operation-specific guidance and NDP.

CHAPTER III
PLANNING AND ASSESSMENT

"Taking away the enemy's anonymity is one of the most powerful joint force capabilities for the Long War."

Admiral E.P. Giambastiani
Vice Chairman of the Joint Chiefs of Staff, 2007

1. General

a. Identity activities are mission enablers. Commanders should incorporate identity activity collection, processing, exploitation, and I2 and/or DOD law enforcement criminal intelligence production in all phases of mission planning. Identity activity planning at the operational and tactical levels is ultimately nested within the higher headquarters' CONOPS. Commanders and staffs use the military decision-making process, and small-unit leaders use the troop-leading procedures to plan and prepare to execute identity activities. Both of these processes have universally understood procedures that apply selected concepts to identity activity planning.

b. Commanders conducting operations that include identity activities should ensure that subordinate unit missions are integrated by task and purpose. For example, conducting a cordon and search or raid can result in identity information and I2 products that facilitates subsequent attacks targeting the threat network. Similarly, technical and forensic exploitation of components recovered from a weapons cache can yield actionable intelligence that allows commanders to target the actors who make up threat networks. The commander ensures the CONOPS clearly describes the identity activities scheme of maneuver and expresses how each element can cooperate to accomplish the mission. Commanders must ensure their forces are properly trained in identity collection, exploitation, and analysis techniques and processes, and that all echelons of leadership have an understanding of how identity activities contribute to and further enable the achievement of mission objectives.

2. Planning Imperatives

a. Planning considerations should incorporate those identity activities that best enable a specific military action or set of actions to accomplish tasks and mission. Planning should detail multiple approaches in employing identity activities as it is adapted to changing circumstances, or enable seamless transition between phases of operations.

b. To properly apply the suitable level of identity activities, deliberate planning should provide a broad framework of the assumptions and conclusions about the OE. It should provide a perspective on who will conduct certain actions, what resources are available, and how it is to be implemented. To effectively execute identity activities, planning should also identify and prioritize actors of concern; cultural sensitivities; existing international agreements to collecting, storing, and sharing personal information; and other nuances. The guidance should identify the countries or organizations that can complement or supplement

US identity capabilities. The plan should also incorporate the transition of identity activities through the six phase joint operation construct (phases 0-V).

c. GCCs and their staffs incorporate appropriate identity activities during the planning, execution, and assessment of major combat and contingency operations as well as security cooperation activities and stability operations. The key planning considerations are:

(1) Plan for the integration and interoperability of identity activities support to operations, security cooperation, and other activities across all phases of the GCCs' TCPs.

(2) Establish intergovernmental cooperation involving identity activities early in the planning process.

(3) Coordinate with operational law staff judge advocates (SJAs) frequently to ensure compliance with DOD policies, international agreements, treaties, and PN laws regarding the collection, processing, storage, and sharing of identity-related information.

(4) Plan for the employment of identity activities, to answer the commander's critical information requirements (CCIRs). The CCMD J-2 should work closely with the national IC components to integrate I2 considerations into theater estimates, orders, and operations.

(5) Ensure that potential threats, known threats, and their supporters are immediately nominated to the DOD BEWL as the authoritative watch list for the command, and when they meet the threshold for national KST watch listing, to the NCTC through DIA.

(6) Establish necessary joint, interagency, and multinational sharing arrangements and service level agreements to support component collection efforts.

(7) Establish theater specific operation policies, procedures, and CONOPS, where appropriate.

d. Commanders must pay particular attention to their environment, influence, and limitations as the ability to collect and exploit identity data can vary greatly based on several key factors:

(1) **Phase of the Operation, HN laws, and Current Rules of Engagement (ROE).** Identity activities may be limited or restricted completely for some mission sets. Capabilities should be employed to the extent allowable by set conditions, with commanders being careful not to exceed their collection and exploitation authorities. Depending on the mission, certain identity data may be collected via different means or elements of identity activities; I2 may not be required, permissible or applicable. For example, one theater may require voluntary participation for identity enrollment, where in another AOR compulsory enrollment may be permissible based on the approved ROE.

(2) **Need for Interorganizational Sharing.** Interorganizational sharing of appropriate identity information will be critical to protecting the US homeland and US interests abroad, deterring and preventing conflict, shaping regional stability, and assuring

allies' and PNs' of our commitment to shared security. The challenge is to find a suitable balance between the growing need to share relevant information and the need to enforce applicable policies to protect certain information.

(a) Increased interagency cooperation is vital in conducting complex contingency operations to bring all instruments of national power to bear on all such operations. Establishing interagency coordination to integrate identity information reduces duplication across the agencies and maximizes the use of limited US resources. GCCs should develop plans policies that delineates the roles and responsibilities in identity activities and incorporates sharing of identity information with interagency partners.

(b) Challenges of globalized international and regional threats have increased the need to dynamically and securely share information among US forces, allied forces, and MNFs. Rules for sharing identity data and associated I2 vary widely among NATO member states, the US, European Union (EU), other PNs, and HNs. Additionally, rules for collecting and sharing identity information are influenced by the citizenship of the individual, the reason the data was collected, and the classification level.

(c) When planning the incorporation of identity activities into missions and operations, commanders must consider the military objective but also who else will need the information in order to support the broader US national security goals. Efforts must be made early in the planning process to ensure identity information is usable and interoperable across various intergovernmental systems and at the lowest classification possible.

(3) **Cultural Considerations.** Joint forces need to demonstrate an understanding of the political, social, economic, and religious dynamics of the OE before executing identity activities. For example, CCDRs should conduct an in-depth cultural analysis, beyond the cursory overview, to identify those cultural attributes of a relevant organization or group, which may pose either short-term or sustained challenges in conducting identity activities. Developing cultural knowledge and understanding and integrating it into operations will mitigate potential challenges in identity collection and determine what attributes that may be sensitive, where identity information is stored, how it is to be used, or with whom the identity information can/cannot be shared.

(4) **Geographic and Technological Constraints.** During an operation's planning phases, commanders must consider the geographic area, environmental elements, and the availability of power and communications equipment for forces operating in the operational area. Utilizing organic communications equipment to reduce the time required to transmit, share, match, and verify identity information is encouraged to the maximum extent possible, as nonorganic equipment may be limited or unavailable in austere operating areas. Commanders should plan for remote operations and determine how to mitigate challenges in collecting and matching biometric data, downloading watch lists, and utilizing DOMEX and forensic reachback capacities. When conditions warrant, the commander may increase reliance on watch lists or allocate specialized communications equipment (e.g., satellites) to the unit. Remote or maritime operations present challenges to ensure sufficient spare equipment and consumables are available and that the maintenance cycle is responsive. Additionally, austere and remote locations may require planning for the evacuation of certain

collected material to preserve, process, and analyze it to extract relevant information in a timely manner. The same may be true of units operating afloat enrolling individuals or exploiting materials found on suspect vessels in a maritime environment. These units may also have a far more difficult time updating watch lists or taking advantage of available reachback capabilities while simultaneously being the most likely to encounter hostile individuals or networks of interest. The unique challenges of the specific OE should be considered in order to plan the right mix of equipment and capability to mitigate these challenges, enhance effectiveness, and maintain the ability to match and share the information as quickly as possible.

(5) **Command Involvement.** When units are tasked to perform an action that involves identity activities, commanders must place an emphasis on the quality and quantity of collections. Identity activities should be incorporated into unit training, unit exercises, and predeployment training as early as possible, when applicable. When deployed, the command should consider appointing an individual or multiple individuals with the appropriate authority and mix of expertise (e.g., law enforcement; intelligence; explosive ordnance disposal [EOD]; chemical, biological, radiological, and nuclear [CBRN]) to coordinate and direct identity activities and fuse, share, and act upon identity-related intelligence or information. This person(s) should serve as the unit's point of contact for follow-ups, reviewing results of identity collection and exploitation and fusing the data to enhance the overall operational picture, identify gaps or shortfalls in collection and analysis, and with appropriate authority, tasking units in order to fill any gaps. This construct will facilitate the sharing of identity information with organizations outside the unit.

3. Operational Approaches

a. There are multiple operational approaches to employ identity activities that a commander can consider based on the strengths, weaknesses, opportunities, and threats of the various actors operating within the OE. The applicability of these approaches depends heavily on the challenges presented by the existing conditions of the OE and the military problems facing the JFC. Commanders should consider each step in the identity activities operational cycle separately when developing their operational approach to ensure each aspect is fully examined. The resulting planning guidance should define the identity activity resources and tactical actions that must be taken to impact the root causes of the military problem and support attaining the strategic ends defined in higher-level guidance.

b. In addition to the tasks defined within the identity activities operational cycle, commanders must consider the conditions, circumstances, and influences that affect the provision of identity activities capabilities, namely the factors that bear on the training and deployment of forces, acquisition and fielding of collection and exploitation capabilities, and the C2 of those elements across the OE. The availability, capacity, and effectiveness of identity activity capabilities can be severely impacted by a lack of forethought and planning related to these factors.

(1) **Collection.** There are three primary approaches to identity activities collection: collections conducted through foreign information sharing partnerships; HN collections enabled by US forces, training, and equipment; and direct collection by US forces and PNs.

In most instances, a combination of two or all of these primary approaches will be used to support military operations. Commanders should remain conscious of the time required to conduct a sufficient collection effort using each approach (or combination thereof) and the impact that will have on supporting exploitation, analysis, and production activities.

(a) Within each operational area, commanders should endeavor to reach a tipping point of collected identities as quickly as possible. A tipping point is the moment at which the required number of unique identities within a given geographic area facilitates a steady stream of repeat encounters of military value. The tipping point for each operational area will be different, depending on the threat faced, and will require a different level of effort for collection. For instance, collections in Afghanistan focused mainly on military-aged males and required the collection of approximately 1.8 million unique identities to reach the tipping point. The tipping point in Operation IRAQI FREEDOM only required the collection of 1.1 million unique identities because of the primarily urban nature of the OE.

(b) System interoperability between US components and PNs is an important consideration. Disparity in data standards can greatly affect the timeliness of data processing activities as well as the future use of the collected data.

(c) Data quality should be a significant priority as it affects processing timeliness and, in some instances, accuracy. The strategic and downstream impacts of poor data quality cannot be understated. Data collected in an operational area through even a single encounter may be used to identify, target, track, interdict, detain, and prosecute threat actors encountered days, weeks, or years later by DOD components, interagency partners, or select foreign allies operating anywhere in the world. JFCs should require all identity activity collectors to meet defined training and certification standards, as appropriate.

(d) Certain types of collection activities may require specialized collection teams. These teams may include low density, high skill set expertise and require significant lead times to be deployed in significant numbers. Commanders should anticipate the need for specialized teams throughout each phase of an operation, and request forces accordingly.

(2) **Processing and Exploitation.** Processing and exploitation can be conducted forward in an expeditionary capacity, through reachback capabilities, or a combination of the two. Forward elements may improve timeliness of response but may limit access to relevant information. These capabilities may also be more expensive to operate and maintain in theater. Reachback elements can provide access to more comprehensive and authoritative repositories but require more time to respond to tactical and operational requests. Forward elements will often have lower throughput capacity than reachback elements but will also likely avoid distraction by other organizational requirements and instead focus primarily on meeting the commander's needs.

(a) C2 of expeditionary elements should be defined early in the planning process. Given the limited capacity of expeditionary elements, multiple force providers serving multiple operational focus areas (e.g., law enforcement, intelligence, C-IED) may seek to deploy expeditionary processing and exploitation capabilities to support the mission. Without sufficient organization and C2 to facilitate unity of action, these capabilities will

likely operate in an unsynchronized, inefficient, and redundant fashion. A clear understanding of the C2 relationship, as well as facilitated integration of force provider capability into the JFC's designated task force (TF) will minimize the expeditionary element's time to reach full operational capability.

(b) The operational needs met by processing and exploitation capabilities will likely change throughout each phase of operation. The results of processing and exploitation activities used primarily to support targeting in early phases may be re-used to support prosecution and rule of law activities in later phases. It is incumbent on the commander to organize and direct the processing and exploitation elements under his command to execute their functions in ways that are mutually supportive to the requirements of both activities. This may mean exploitation activities executed to support intelligence operations are conducted anticipating future chain of custody requirements. Similarly, activities conducted to enable detainee processing, management, and prosecution may also need to enable follow-on targeting missions, interviews and interrogations, and source operations.

(c) Common information management and sharing architectures are a vital component of the processing and exploitation function. Follow-on analysis and reference activities require robust secure yet accessible databases that allow for ready discovery and usability of processing and exploitation results.

(3) **All-Source and/or DOD Law Enforcement Criminal Intelligence Analysis.** I2 production activities can be conducted at the tactical, operational, and strategic levels to support a broad variety of joint functions including protection, fires, and movement and maneuver throughout the OE. Law enforcement organizations conduct DOD law enforcement criminal intelligence analysis to support investigations, identify and track criminals, assess criminal informants, and support prosecution activities. I2 and DOD law enforcement criminal intelligence production provides fundamental underpinnings to support the commander's efforts to shape the OE, deter threat actors and networks, reestablish safe and secure environments, and develop or strengthen the legitimacy of HNs, while protecting the force, enhancing cybersecurity, and reinforcing HD efforts. Commanders should clearly define the focus areas of I2 and DOD law enforcement criminal intelligence analysis at each echelon to maximize economy of effort. Roles and responsibilities for all-source and DOD law enforcement criminal intelligence production should be assigned from Service intelligence centers, joint intelligence centers/joint analysis centers and DOD law enforcement agencies, CCMD staff and Service staffs, as appropriate, across TF and brigade intelligence cells and criminal investigative components, and down to individual unit support elements. Clear guidance and direction will help ensure a sustainable distribution of effort between strategic-theater production (e.g., JIPOE, criminal indictments), operational assessments (e.g., named areas of interest [NAIs]), and tactical support (e.g., watch listing, warrant support packages).

(4) **Production and Dissemination.** Clear standards and guidance for production and dissemination is critical for the effective employment of identity activities. Given the sensitive nature of identity information and its value to almost any operational effort (including nefarious activities like extra-judicial killings and sectarian violence), commanders must ensure that adequate processes and safeguards are in place to facilitate the

sharing and use of identity information and their corresponding I2 and/or DOD law enforcement criminal intelligence assessments in legal, responsible, and ethical ways.

(a) US forces, HN forces, and MNFs will collect much of the operationally relevant identity information and materials overtly. However, a majority of the associated derogatory information discovered during the all-source analytic process will be classified or deemed law enforcement sensitive. To make these assessments operationally useful, the commander must dictate and actively enforce a requirement for releasable tear lines and unclassified products. Identity information, related reports, and I2 and/or DOD law enforcement criminal intelligence assessments must be usable the combat formations as well as in the planning office.

(b) Even when information is originally unclassified (e.g., biometric match reports), measures must be taken to ensure it cannot be used in inappropriate ways. Information sharing with HN personnel and foreign partners must be conducted in compliance with US law and the laws of the receiving partner. Commanders should establish robust foreign disclosure processes designed to review identity files and related reports, even when unclassified, to ensure the receiving entity cannot use the provided information in other than intended ways. Formal risk assessments should be conducted prior to the initiation of sharing activities to determine the vulnerabilities to US identity activity capabilities, operations, and national reputation should the provided information be used for nefarious purposes or be further shared with unauthorized parties.

4. Planning Identity Activities

a. Planning for integrated and synchronized identity activities should address all levels of warfare. The actions at the strategic level include the coordination of all instruments of national power, collaboration with the CCMDs to collect and share information using responsible and appropriate mechanisms and safeguards to inform a wide array of missions and activities, and the establishment of technical means and standards to ensure the enterprise can support the timely access, discovery, and use of identity information and analysis. At the CCMD level, the identity activities plan provides guidance for identifying, characterizing, and targeting threat actors and elements of the threat network, effectively monitoring and assessing threat actor/network activities, training the force in identity activities, and transferring equipment and capabilities to participating coalition and MNFs partners and the HN to support operations. Planning for identity activities should be an integral part of the overall TCP and subordinate plans. The actual planning and conduct of theater identity activities will depend on the security agreements with HNs, capabilities of HN forces, time phasing of available US capabilities, and the quality of the JIPOE assessment. The identity activities requirements will be established by the JFC. For identity activity operations to be effective across all levels of warfare, they must be viewed in the context of the larger whole-of-government operation or campaign plan and integrated across all staff sections and functional areas.

b. Identity activity planning is initiated in anticipation or receipt of a mission, as a branch or sequel to an ongoing operation, as part of a base order, or as part of a unit standard operating procedure. Information gained from identity activities can lead to a follow-on

operation. Identity activities support the commander's decision-making process by providing information needed to satisfy information requirements. The staff adjusts the collection plan if the information requirements are not satisfied, which often leads to further identity activities.

c. The requirement to collect materiel, answer information requirements, conduct on-site analysis, and develop the information gained is implied in all operations when not directed as a specified task. Identity activities include implied tasks, such as biometric enrollment, forensic collection, material preservation, and intelligence or DOD law enforcement criminal intelligence analysis, which are supporting tasks needed to meet the purpose of the activity.

d. Identity activities are typically conducted as part of one or more of the following actions:

(1) CTN.

(2) Targeting/persistent intelligence, surveillance, and reconnaissance.

(3) Raid/cordon and search.

(4) Access control.

(5) Population management/population mapping.

(6) Site exploitation.

(7) Law enforcement/support to rule of law.

(8) Census operations.

(9) Population resource control.

(10) Intelligence activities.

e. Planning involves an analysis of the organizational structure and supporting assets (direct and general) available to perform the task, identification of constraints, and an assessment of risk.

(1) Identity activities require a clear understanding of the personnel available, their level of training, and in what capacity they can support identity activity tasks. Maneuver Service members trained in forensic collection tasks provide a different level of capability than a weapons intelligence team trained in specialized search techniques and equipment. Additionally, equipment available (e.g., biometric collection devices, presumptive testing kits, expeditionary exploitation equipment) influences COA development. Commanders consider the time available for identity activity planning and the time sensitivity of the collected information, materiel, and personnel detained on site. The availability of supporting agencies that provide enabling capabilities, such as information processing,

technical analysis, forensic collection and exploitation, and render safe capabilities, also influence identity activity planning and COA development. Commanders, coordinating staffs, and liaison officers identify capabilities and limitations of the assets associated with their respective area of expertise. Commanders also need to know about exploitation-specific information systems and which are the quickest for receiving feedback.

(2) Identity activities must be planned and executed within the physical, diplomatic and political constraints of the operation. A constraint is a restriction placed on the command by a higher command. A constraint dictates an action or inaction, thus restricting the freedom of action a subordinate commander has when planning. Examples of constraints for identity activities planning include, but are not limited to, ROE, search restrictions relating to gender, and rules for the use of force (RUF). Constraints affect COA development of both the parent unit and subordinate elements. Constraints are considered as tasks and included in the coordinating instructions in operations orders to account for the impact on identity activity planning and execution.

(3) Leaders at all echelons conduct risk assessments before each tactical collection or exploitation activity. A risk assessment increases the staff's awareness of anticipated or unknown risks. Risk assessment also allows for planning measures that mitigate the risk to military personnel. Leaders on-site use risk assessment to avoid or mitigate hazards and risks. The goal of risk management is to implement controls that remove hazards or reduce the residual risk to an acceptable level. Commanders and leaders at all levels need to know the hazards associated with identity activities. Risk awareness allows commanders and leaders to weigh hazards against the anticipated value of the information gained. There are instances where the collection, handling, and processing of information and materiel is of paramount importance and can potentially place personnel at risk. Commanders and leaders minimize risk by establishing mitigation measures and safety guidelines before conducting tactical collection and/or exploitation.

f. The CCIRs and other information requirements help focus the staff's planning efforts. The CCIRs can be time-sensitive, especially when related to targeting or CTN missions. The CCIRs are specific enough to assist the staff in understanding what personnel and equipment are required for identity activity support to a specific action. Staffs recommend intelligence requirements for designation as PIRs in an effort to gain additional information about the threat and the OE. Lessons learned from recent operations show that some missions sets require civil information and sociocultural analysis as a PIR.

g. An information collection plan links the collection effort to the commander's information requirements. Often, time constraints shape the need for information. Within an area of operations, identifying areas of interest helps establish the scope of the collection effort. Considerations may include the scale and complexity of the area and confirmation or exclusion of the presence of WMD, booby traps, hostile forces, or civilians.

h. Whether conducting identity activities is the primary mission or planned as a subsequent or secondary task, identity activities COA development follows the same considerations of any planning effort. When developing COAs, the commander and staff array their forces and task-organize assets to perform specific identity activity tasks.

Enablers are sometimes required to augment the collection and/or exploitation element to provide specialized capabilities to the executing unit(s). When establishing the support relationships, commanders consider the supporting distance and prioritization of use for specialized supporting agencies.

5. Integrating Identity Activities into the Joint Planning Process

The joint force typically conducts identity activities within the context of a broader operation or campaign. However, in certain instances the JFC may choose to conduct focused identity activities to support elimination or neutralization of a threat in a specific area. In either case, commanders and their staffs must integrate identity activities into JPP to realize their maximum operational effectiveness. Planning for the collection of identity information and data, as well as the exploitation of that data, should be included within all operational planning processes and account for all events, from departure of friendly lines to reentry into friendly operational areas or extraction.

a. **Planning Initiation.** During planning initiation, the commander and his staff define how identity activities can be leveraged within their operations. Particularly when planning for crises, the JFC and staff will perform an assessment of the initiating directive to determine the time available until mission execution to gather identity activity capabilities, the current status of intelligence products and staff estimates related to threat actors and networks (e.g., JIPOE, BEWL), and other factors relevant to the specific planning situation. Initial planning guidance should specify time constraints, outline initial DOD and interagency coordination requirements, or authorize movement of key identity activity capabilities within the JFC's authority. Additionally, the commander and his staff may seek to enhance their current understanding of the OE, the problem, and the initial operational approach for the campaign or operation.

(1) The J-2 develops the intelligence estimate which includes all-source analysis fused with identity information and data, as well as the identification of persons of interest, KSTs, and high-value individuals (HVIs).

(2) The civil affairs (CA) officer develops the civil considerations estimate and determines whether the local population will comply or resist identity information and data collection, to include biometric enrollments.

(3) The commander and staff develop initial information requirements, to include the need for identity activities that support the discovery of persons of interest and/or HVIs.

(4) The commander and staff develop the initial reconnaissance and surveillance guidance, to include identity information and data collection at ports of entry, troop assembly areas, along main supply routes, and other NAIs.

b. **Mission Analysis.** The commander conducts mission analysis to develop and focus staffs' and subordinate commanders' thinking and efforts to achieve the goals and objectives of the operation. The commander assesses the guidance from higher authority, analyzes the OE, integrates the operational approach, and produces a restated mission and commander's

intent and planning guidance. Identity activities should be effectively integrated into the mission analysis function to successfully enable military operations.

(1) **Determination of Specified, Implied, and Essential Tasks.** The staff must have knowledge of the standard identity activity and their functions to determine whether or not the purpose of the operation and the expected OE will make them essential to success and therefore explicitly stated in the restated mission. If not specified, identity activity collection, exploitation, and analysis should be considered implied tasks across all phases of the operation.

(2) **Force Allocation Review.** The initial force allocation review will reveal the capabilities, limitations, and training levels of the joint force. When facing an asymmetric threat, in most cases, units will require dedicated identity activity enablers. These are organizations, systems, or training that will best allow a unit to operate safely, to use intelligence resources, and to effectively engage targets. Force allocation analysis must consider the adequate allocation of collection equipment, the capacity and accessibility of expeditionary processing and exploitation capabilities, and the availability of I2 and/or DOD law enforcement criminal intelligence-trained analysts capabilities to support mission needs, and arrange for augmentation as required. The JFC's logistics directorate of a joint staff (J-4) assesses whether there is sufficient identity activity equipment to support commander's vision and intent.

(3) **Information Requirement Development.** The commander and his staff develop the initial CCIRs and essential elements of friendly information (EEFIs). Identity activity integration into the CCIRs and EEFIs will be determined by the commander's and staff elements' guidance to include: reconnaissance guidance, deception guidance, fire support guidance, mobility and counter mobility guidance, security and protection measures, the time plan, and the types of rehearsals to conduct. The JFC's J-3 leads the development of the initial information collection plan and should include identity activity collection requirements.

(4) **JIPOE.** The JFC's J-2 leads the JIPOE process. The J-2 also identifies information requirements and intelligence gaps and evaluates assets for information collection to include identity activity requirements (e.g., linguist requirements, CI and HUMINT source-vetting requirements, contractor vetting requirements, physical security requirements, force protection vulnerabilities) from all joint staff sections.

(a) The basic JIPOE process provides a disciplined methodology for analyzing the OE and assessing the impact of that environment on adversary and friendly COAs. However, depending on the situation, additional, specialized, graphic displays may be developed to support and provide greater clarity to the JIPOE effort.

(b) The following discussion illustrates some common JIPOE specialized products relative to identity that could be used to support mission analysis.

1. **Legal Status Overlay.** Legal status overlays may be constructed to depict the impact on the OE of established or planned ROE and international law, including the law of the sea. These overlays display actual or potential "no-strike" areas.

2. **Religion, Race, and Ethnicity Overlay.** Religion, race, and ethnicity issues often contribute to conflicts. Religious, race, and ethnicity overlays depict the current ethnic and religious makeup of an operational area. These overlays can also display any specific religious-, racial-, or ethnicity-specific areas and any zones of separation agreed upon by peace accords. These three overlays may be separate or combined.

3. **Perceptions Assessment Matrix.** Although the perception of an HN's population may be difficult to gauge, it is key to successfully planning, executing, and assessing joint operations. In-depth knowledge and understanding of the national, regional, and local cultures, norms, moralities, and taboos are needed to understand the OE and reactions of the population to friendly operations. Perceptions assessment matrices may be used to characterize and summarize public perceptions regarding various conditions.

4. **Activities Matrix.** Relationships (links) in large data sets are established by similarities between the nodes. People are identified by their participation in independent activities. When graphed, pairs who have engaged in the same activity (columns with dots) are designated with a link on the network analysis diagram.

5. **Association Matrix.** An association matrix portrays the existence of an association, known or suspected, between individuals or entities. Association matrices provide a relatively one-dimensional view of the relationships among entities, but can be used by analysts to help focus their attention on entities and relationships requiring greater detail.

6. **Link Diagram.** Link diagrams graphically depict relationships between people, events, locations, or other factors deemed significant in any given situation. Link diagrams help analysts better understand how people and factors are interrelated in order to determine key links.

(5) **Communications Architecture.** The JFC's J-6 assesses network and communication requirements based on identity activity collection requirements. Personnel involved in identity activities must identify communications requirements in order to be included in the information network planning and to ensure the appropriate data transmission architecture is in place to support forward and reachback biometric matching activities. These requirements should include data sharing with HN and MNFs, and support to I2 and/or DOD law enforcement criminal intelligence production activities.

c. **COA Development.** Identity activities should be addressed at the appropriate level in each COA and describe who will conduct the identity activity, what type of identity activity/function will occur, when it will begin, where it will occur, why the identity activity is required (purpose), and how it will occur (method of employment). Commanders should seek to integrate both multifunction and specialized identity activity collection elements within each COA to maximize coverage and availability of forces to meet mission

objectives. Whenever possible and appropriate, mission planners should design for and enable PN forces to lead identity activity collection efforts.

d. **COA Analysis.** During COA analysis, planners should take into account sensitivities and potential reactions among the target population. A SJA review might be necessary to determine the permissibility of identity activity information and data collections in the OE and among the target population in accordance with existing policies and agreements with the HN.

e. **COA Comparison and Approval.** Staff should consider how identity activity can be effectively compared between COAs and how those comparisons can illuminate risk. Since identity activities can be disproportionately affected by sociocultural dynamics, HN and PN legal limitations, and technical constraints, thoughtful consideration should be given to the advantages and disadvantages of including or eliminating identity activities, who should conduct identity activities, what types of collection and exploitation should be included, and the political and cultural risks of conducting identity activities within each COA. Upon selection of the preferred COA, JFCs should ensure relevant interagency partners, country teams, and DOD components are notified and/or coordinated with on the identity activities aspects of the COA, as appropriate or required.

f. **Developing a CONOPS.** During CONOPS development, the commander should determine and express the best arrangement of simultaneous and sequential identity activities required to accomplish the assigned mission in sufficient detail to allow for the identification of specified and/or implied tasks.

g. **Plan or Order Development.** Identity information and data collection and exploitation should be included in every operation order to the extent appropriate for the operation. Identity activity considerations should be discussed in any applicable place in a plan or order but should be considered for the following annexes and appendices: annex B (Intelligence); annex C (Operations); annex E (Personnel); annex F (Public Affairs); annex G (Civil Affairs); appendix 3 (Information Operations) to annex C (operations); appendix 14 (Force Protection) to annex C (Operations).

6. Assessment of Identity Activities

a. Commanders and their staffs must conduct assessments of identity activities as they would any military operation or activity to determine if they are creating the desired effects. Threat networks will adapt visibly and invisibly even as collection, analysis, and assessments are being conducted. Assessments over time that show trends are much more valuable for identity activity planning and operational support than a single snapshot over a short time frame. Over longer periods of time, information can be pieced together and changes in threat network organization, structure, composition, functions, and operational capabilities can be identified and analyzed. This is particularly valuable for TCP development and in ongoing phase 0 and phase I operations. GCCs develop their theater strategies by analyzing events in the AOR and developing options to set conditions for attaining strategic end states. When a joint force is employed, it will at a minimum have a baseline of the threat network(s), its characteristics, and behaviors based on phase 0 operations. Assessment of identity activities

is part of the larger operation or campaign assessment and can also support indicator monitoring and measuring effectiveness.

b. Identity activities require a greater application of operational art due to the complexity of the human environment of the OE. Likewise, identity activity assessments demand staffs conduct analysis more intuitively and consider both anecdotal and circumstantial information. Tactical unit reporting such as patrol debriefs and unit after action reports, when correlated across an OE, may provide the most valuable information on assessing the impact of identity activities.

c. Commanders and their staffs should conduct assessments through a continuous process of evaluation and feedback, in which metrics relating to performance and effectiveness of tactics, techniques, and procedures (TTP), systems, and networks are collected and used to assess the entire range of identity activity-related capabilities. This process allows commanders and staffs to improve the effectiveness of identity activities-related capabilities, refine identity data collections, augment I2 production requirements and priorities, and capture best practices and lessons learned. Timely collection and dissemination of lessons learned can specifically influence the next iteration of exploitation or collection activities, supporting the primary goal of avoiding missed opportunities to protect the force or eliminate threats from the OE due to ineffective processes or missed matches against known and discoverable identity data.

d. An identity activity assessment process can take many forms but all versions typically incorporate four basic tenets: assemble a team of experts to develop indicators, combine different types of indicators to develop a more complete assessment picture, assign weights on multiple axes of the assessment (i.e., by indicator/effect) to ensure that the assessment matches the JFC's priorities, and synchronize assessment timelines so the results flow into higher headquarters' planning processes.

(1) Commanders are encouraged to use a multi-organizational assessment working group approach to develop assessment indicators, which provides the benefit of expert perspectives throughout the staff and subordinate commands, including the concerns of assigned interagency and MNF personnel. This ensures that the selected questions reflect the priorities of the command and its leadership.

(2) Identity activity assessments should use data from varied sources and employ numerous indicators to ensure the assessment is not dominated by one type of data and represents the full operational view.

(3) The assessment should measure the full array of identity activities tasks and functions across the operations, intelligence, and law enforcement areas.

(4) The commander should weight each indicator so his most important priorities are reflected in the assessment.

(5) Finally, the assessment process should align to higher headquarters' planning processes, so the assessment results can shape and influence changes in strategy and planning.

e. Integrated successfully, assessment in identity activities will:

(1) Depict progress toward creating desired effects, achieving objectives, and attaining the commander's military end state(s).

(2) Deepen understanding of the OE, JIPOE, and the ongoing intelligence process provides the JFC the primary understanding of the OE. Assessments of identity activities can provide additional understanding and greater knowledge about threat actors and networks, and how operations may be impacting their ability to operate effectively.

(3) Inform commander decision making for operational design and planning, prioritization, resource allocation, and execution. Since identity activities require a high degree of operational art, the contribution of assessments is particularly relevant.

(4) Produce actionable recommendations that inform the commander where to devote resources along the most effective lines of operation and lines of effort.

See Appendix C, "Assessment Indicators for Identity Activities," for more information.

7. Using Identity Activities to Support Operational Assessment

a. Commanders continuously observe the OE and the progress of the operation; compare the results to their initial visualization, understanding, and intent; and adjust operations based on this analysis. Staffs monitor key factors that can influence operations and provide the commander timely information needed for decisions. Identity activity capabilities can directly support operational assessment, providing a mechanism to monitor key indicators and measure effectiveness and performance.

b. During execution, assessment actions and indicators help commanders adjust operations and resources as required, such as determining when to execute branches and sequels and make other critical decisions to ensure current and future operations remain aligned with the mission and military end state. Threat networks thrive because of conditions that support their existence and their operations. For example, some threats are supported and concealed by a local populace. However, efficient use of identity activities can deny a threat anonymity and the ability to blend into society. Additionally, military actions and objectives in the OE can be affected by the actions of a wide variety of entities. These actors include not only the JFC's interorganizational participants but also the civilian population, neutral non-partner organizations in the joint operations area (JOA), and other countries outside the JOA in the CCDR's AOR. Identity activities provide a viable mechanism to identify, assess, and monitor these entities throughout all phases of the operation.

c. Commanders and staffs at all levels develop various operational assessment indicators to track the organization's progress toward mission accomplishment. These indicators include measures of effectiveness (MOEs) and measures of performance (MOPs).

(1) The intent in developing MOEs is to identify indicators confirming that military operations are producing desired effects. Identity activities "hits" can serve as MOE

indicators of observable, measurable, system behaviors or capabilities. How successfully various I2 products satisfy I2-related PIRs can serve as MOP indicators of the effectiveness of identity activities. These indicators help to focus intelligence collection planning. When developed, identity activity-based indicators can inform planning and execution of intelligence collection activities.

(2) MOPs typically focus on task accomplishment. MOPs are criteria used to assess friendly actions tied to measuring task accomplishment. They are a primary element of battle tracking and are associated with objectives rather than end-state conditions. An example of a MOP is the capture of a high-value target on the DOD BEWL.

(3) Identity activity indicators help commanders and staffs determine whether they are taking the proper actions to attack threat actors and networks operating in their operational area. For example, a reduction in the number of foreign fighter encounters is a straightforward indicator of success. Some indicators may be more subjective in nature, however. The willingness of local elders to work with the government and submit their community to identity activity screening is an example of a subjective assessment that requires professional military judgment to determine meaning. It may demonstrate the threat is exerting less control and fear over the population or it may simply imply a socio-cultural willingness to participate in local security activities. Identity activities can also help monitor indicators of success, such as reductions in a certain tactic employed by the threat network. Enemy shifts in tactics made in response to joint force operations may be a clear indication the JFC is creating the desired effects. Commanders should leverage identity activities to monitor these affects and use them to enhance follow-on planning and decision-making processes.

8. Organizing Identity Activities Within the Joint Force

a. **Staff Support to the CCDR.** Every GCC and Commander, USSOCOM has established formal CCDR guidance (e.g., policy, TCPs, CONOPS) and a dedicated office to manage and integrate identity activities into their planning and engagement activities. This office is responsible for ensuring the commander understands the identity activity tactics, techniques, capabilities, needs, and limitations of the component parts of the joint force. It works to guide and inform lower echelons to ensure planning and employment consistency and unity of effort. Primary staff responsibility for identity activities varies with each CCMD. It is important to remember that identity activities support missions across the conflict continuum require a cross-functional effort. Regardless of which element is assigned as the office of primary responsibility, the following responsibilities are maintained:

(1) **CCMD J-2.** The CCMD J-2 assists the JFC in developing regional and theater collection strategies; planning identity activities within operations and campaigns; and tasking intelligence assets, when required, to support identity information and forensic collection, processing, exploitation, all-source analysis, and I2 production within joint and multinational OEs. The CCMD J-2 determines the intelligence requirements relevant to identity activities and provides direction to ensure unity of the intelligence effort to support the commander's objectives; and is responsible for leveraging national intelligence capabilities, optimizing the utilization of joint force intelligence assets supporting identity

activities, and identifying and integrating additional reachback intelligence resources. If needed, the J-2 can appoint an identity activities or I2 program manager, as appropriate, to coordinate and oversee identity activities/I2 production activities within the CCMD. The CCMD J-2 is ultimately responsible for employing identity activities, as appropriate, to analyze all relevant aspects of the OE, identify relevant threat actors and networks, answer intelligence collection requirements, determine adversary capabilities, and estimate adversary intentions. Furthermore, the J-2, through the application of I2, links threat personnel to threat activities, collected material, and signatures. The CCMD J-2's reliance on non-intelligence collection, processing, and exploitation capabilities necessitate a close collaboration with the CCMD J-3.

(2) **CCMD J-3**. The CCMD J-3 is responsible for identity activities planning and integration and assists the CCDR in the direction and control of operations. Its work begins with initial planning and extends through the integration and coordination of joint operations. The CCMD J-3 may establish an identity activities operational planning team (OPT) to provide day-to-day staff integration planning, coordination, synchronization, and execution of identity activities in support of TCPs and operational missions. The OPT should include an identity activities program manager, I2-trained all-source analysts, an identity operations manager (IOM), a forensics technical representative (FTR), and representation from the CCMD J-2. The identity activities program manager represents the CCMD office of primary responsibility and is responsible for overall day-to-day management as the command's principle staff advisor on identity activity capabilities and efforts. The IOMs integrate and synchronize theater special operations command (TSOC) identity activities planning and execution with the GCC. The FTR is responsible for the daily synchronization of forensic exploitation activities and coordination across the CCMD staff. The CCMD J-2 representative supports the CCMD J-3 in effectively planning, organizing, and employing of identity activity capabilities to meet the JFC's needs.

(3) **CCMD J-4.** The CCMD J-4 develops logistics plans and coordinates and supervises supply, maintenance, repair, evacuation, transportation, and related logistics for identity activities capabilities and equipment. Because identity activities equipment fielding and logistics support is primarily a Service responsibility, the thrust of CCMD J-4 activities is to coordinate Service programs and integrate them with the JFC's concept of support. When directed, the CCMD J-4 may also manage the CCDR's SSA activities and programs.

(4) **CCMD Plans Directorate of a Joint Staff (J-5).** The CCMD J-5 is responsible for integrating identity activities into long-range planning and planning security cooperation activities, as appropriate. It prepares campaign, concept, and operation plans and facilitates engagement with the various embassy country teams to develop country plans. The CCMD J-5, in coordination with the CCMD identity activities office of primary responsibility, the JS J-5, appropriate OUSD(P) country desk officers, and the relevant embassy country teams identifies, proposes, plans, negotiates, and staffs all identity activity-related information sharing arrangements with PNs.

b. **Staff Support to the JTF**

(1) **JTF J-2.** The JTF J-2's intelligence priorities and efforts are driven by a need for a holistic understanding of the OE. The JTF J-2 organizes and directs identity activity collection, coordinates processing and exploitation activities, and manages I2 production and dissemination. The JTF J-2 supports JTF J-3/J-5 planning efforts and the execution and assessment of identity activities. As required, the commander, JTF may elect to integrate the identity activity responsibilities into day-to-day staff functions, or establish a JTF joint force exploitation staff element (J-2E), in coordination with the JTF J-3, to plan and manage exploitation assets. A JTF J-2E is established as necessary to integrate and synchronize disparate theater-level military, intelligence, law enforcement, multinational, and HN collection, exploitation, analysis, and dissemination capabilities and processes. The decision as to the type of intelligence staff element required will be based on the scope and breadth of the mission assigned to the JTF.

(2) **JTF J-3.** The JTF J-3 assists the commander in directing and controlling identity activities throughout each phase of an operation. In this capacity the JTF J-3 plans, coordinates, and integrates identity activities into operations, typically in concert with the JTF J-2, higher headquarters, and JTF component operations directorates. The JTF J-3 works closely with the rest of the staff to recommend identity activity-related material for inclusion in the commander's intent so it is captured in planning, informs the commander's decision-making process, and contributes to the execution and assessment of operations. JTF J-3 functions typically consider the integration of interagency, multinational, NGO, and IGO identity activity capabilities and initiatives.

(3) **JTF J-4.** The JTF J-4 helps the commander manage the provision of identity activity logistics to the joint force. The JTF J-4's concept of logistic support often involves coordination with the HN, private contractors, and interorganizational partners to effectively execute deployment, servicing, and transportation of identity activity equipment, capability, and materials around the theater of operations. PN and HN support in these areas, through formal acquisition and cross-servicing agreements, can significantly affect the logistics concept and the CONOPS.

(4) **JTF J-5.** During execution of current operations, the JTF J-5 focuses on integrating identity activities into future plans, which are typically for the next phase of operation or sequels to the current operation. The JTF J-5 also supports the integration of identity activities into the JTF's future operations planning effort, which normally occurs in the JTF J-3.

c. **TF Support to a TF.** A JFC may establish a subordinate TF to coordinate and manage the planning, execution, and assessment of identity activities throughout each phase of an operation. Identity activity TFs are organized as a joint element of the joint force, with staff augmentation drawn from each Service component. Directive guidance for the TF typically comes from the JFC; however, the TF must maintain a direct relationship with the GCC's staff and the Service component commands to operate effectively.

(1) **TF Commander.** The TF commander is responsible for supporting all operational-level identity activity planning activities in the operational area. The TF commander supports intelligence and maneuver units in integrating identity activities into

their daily operations and deconflicts their collection, exploitation, and analysis efforts to ensure there is no unneeded redundancy or overlap across the joint force. The TF commander is also responsible for managing the operational area-wide identity activities information architecture, training operators in theater, and interpreting the intelligence gained from collection and exploitation activities to support the JFC's decision cycle.

(2) **TF J-2.** The TF J-2 manages the TF's I2 production cell and develops multi-intelligence products to answer the CCIRs and PIRs of the higher headquarters. He directly supports JFC and GCC's J-2 elements in the development of their assessments, estimates, and intelligence products related to the operation. If delegated by the JTF J-2, the TF J-2 is responsible for managing the watch listing efforts within the JTF's operational area. The TF J-2 also provides additional I2 production training for CF analysts and integrates with USSOCOM I2 production elements supporting the JFC's operations. Identity activity TF J-2s must have a firm understanding of all available identity activity deployed, expeditionary, and reachback capabilities and the intersections, overlaps, and progression of tactical-level collection, exploitation, analysis, and production to strategic-level capabilities, missions, and production efforts.

(3) **TF J-3/J-5.** The TF J-3 and J-5 form the core of the identity activities TF and are often combined into a single element, depending on the size and scope of the operation. The TF J-3/J-5 must be fully cognizant of all identity activity capabilities available to support the operation and have a strong relationship with both JFC and GCC planners. In operations conducted in support of an HN, direct coordination with the GCC foreign policy advisor is also prudent. Primary functions include planning and integration of identity activities within and across all operational phases, communications synchronization activities with HN and PN forces and the local population, and key leader engagements (KLEs) related to the execution of identity activities across the operational area. The J-3/J-5 should maintain a comprehensive understanding of the political environment and work with HN and PNs to influence their operational planning efforts. The TF J-3/J-5 works in concert with the TF J-2 to conduct identity activity planning, advise the JFC, and effectively coordinate and manage the employment and sustainment of identity activity capabilities to meet operational objectives.

(4) **TF J-4.** The TF J-4 manages the logistical aspects and growth of the TF during an operation, including lodging, equipment, and resupply. The TF J-4 also manages the transport of equipment, TF personnel, and collected materials throughout the OE.

(5) **TF J-6.** The TF J-6 works to establish and maintain a joint and, where appropriate, multinational architecture within a secure networked environment. The TF J-6 manages any in-theater database, as well as the reachback communications interfaces and mechanisms. The TF J-6 maintains the critical link between units collecting and using identity information and I2 in a tactical environment and the processing, exploitation, and analysis capabilities supporting their operations at the operating base, regional support element, or continental US hub.

(6) **MNF Elements.** Within a multinational environment, the TF can include one or more multinational partners to support planning, execution, and assessment activities.

These elements can serve as liaison to MNF or be assigned as part of the leadership at the discretion of the JFC. Regardless of the role, it is important to identify and understand the various constraints PNs may operate under, created by their individual national laws, policies, and ROE.

(7) **HN Elements.** Whenever possible, the TF commander should seek to include HN elements within their organizational structure. HN elements can provide an increased level of local legitimacy in planning and executing identity activities, based on their high degree of understanding of local politics, custom, and population groups.

(8) **Interagency Elements.** As appropriate, the integration of interagency partners into an identity activities TF can create a valuable bridge between organic identity activity capabilities and the strategic reachback capabilities of the national security community. The knowledge, experience, and authorities of these interagency partners can greatly enhance the effectiveness of identity activities executed across the various phases of operation.

(9) **Legal Support.** Identity activities TFs do not typically maintain their own special staffs. All legal support for TF operations should be coordinated with the higher headquarters legal staff.

CHAPTER IV
ORGANIZATIONAL ROLES, RESPONSIBILITIES, AND COMMAND RELATIONSHIPS

1. General

a. This chapter discusses the national, interagency, IC, DOD, and operational partners that have a role in identity activities, and highlights their authorities, responsibilities, functions, and capabilities that affect, support, and/or enable the JFC's ability to make use of identity activities.

b. When planning or executing identity activities in support of a military activity or operation, a JFC should identify and leverage all available identity activity capabilities. However, exercising the full power of identity activity capabilities requires a coordinated whole-of-government effort. DOD recognizes that during shaping operations other interagency partners may be the USG lead agency with DOD in a supporting role. To formally coordinate with interagency partners, CCMDs identify identity programs and activities of concern to the JS and OSD. OSD facilitates interaction among CCMDs and interagency partners at the national-strategic level. CCDRs may also use established interagency relationships to increase their success in identity activities.

c. In an active combat theater, JFCs coordinate and cooperate with multinational partners to execute identity activities. With numerous stakeholders in the identity activity mission space, it is critical that unity of effort is achieved and the roles, responsibilities, and authorities of the numerous organizations are understood by the JFC. JFCs should consider the capabilities and responsibilities of the organizations in this chapter when defining command relationships and coordinating interorganizational activities.

2. United States National Organizations, Responsibilities, and Relationships

a. Identity activities at the operational and tactical levels often benefit directly from the combined capabilities of the USG. Coordination between DOD and other USG departments and agencies is critical to the success of identity activities against the global VEO, transnational organized crime, CI, and weapons proliferation threats. During shaping, identity activities are normally led by a department or agency other than DOD. In many cases, the JFC will be supporting another USG department or agency that may be supporting a PN or IGO.

b. The majority of interagency identity activity-related programs and contributions occur as day-to-day activities in what DOD identifies as phase 0 activities, which include ongoing operations and activities such as security cooperation. Since there are a number of different organizations within the USG that contribute to identity activities, it is important to develop some level of mutual awareness of their roles and capabilities to identify potential areas for cooperation.

(1) The NSC manages the interagency process with respect to identity activities for all national security-related issues and certain selected actions. The interagency process is

designed to advance the President's policy priorities and to serve the national interest by ensuring that all agencies and perspectives that can contribute to achieving these priorities participate in making and implementing policy. Thus, the NSC is the key integrator of the President's whole-of-government identity management policies and strategies, which requires interagency coordination at the principals committee, deputies committee, and supporting interagency policy committees (IPCs) and the efforts of the NSC staff. The key IPCs for identity activities are the Biometrics and Identity Management IPC and the Watchlisting and Screening IPC, which are both led by the Special Assistant to the President for Transborder Security. The Biometrics and Identity Management IPC oversees the interagency *Governance Structure for International Engagement on Identity Information*. This plan sets forth the framework for prioritizing outreach, engagement, and sharing of identity information with foreign partners as well as establishes an interagency governance structure for its implementation. All formal military engagements related to identity activities are subject to this plan.

(2) **Department of Justice (DOJ).** The Attorney General investigates acts or incidents that may constitute a violation of federal laws, including acts of terrorism, the use or threatened use of WMD, and the export of strategic commodities and technology. Much of this investigation authority has been delegated to the FBI and the DEA. DOJ provides legal oversight and support for strategic-level identity activities like terrorist watch listing and screening, identification and screening of national security threats, and US participation in the International Criminal Police Organization (INTERPOL).

(a) **FBI.** The FBI is the lead federal agency for investigating terrorism, transnational organized crime, and WMD crimes. The preemptive focus of these efforts requires the FBI to use its investigative and analytical capabilities, to identify potential suspects, targets, and threats before an attack occurs. The FBI maintains several authoritative biometric databases, operates the TEDAC, and maintains oversight and encounter management of the National KST Watch List through the Terrorist Screening Center. The FBI also supports partner capacity and capability building and identity information sharing through its Global Initiatives Unit. The Army's DFBA, USSOCOM, and the Defense Threat Reduction Agency's Joint Improvised-Threat Defeat Organization (JIDO) closely partner with the FBI to enhance the identity activities support they provide to the JFC.

(b) **Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF).** The ATF protects communities from violent criminals, criminal organizations, the illegal use and trafficking of firearms, the illegal use and storage of explosives, acts of arson and bombings, acts of terrorism, and the illegal diversion of alcohol and tobacco products. ATF agents may participate in military operations at the direction of the President or at the request of SecDef. DOD actively leverages ATF expertise in explosives exploitation and analysis and their related CTN activities. ATF I2 and law enforcement criminal intelligence products feed operational intelligence and criminal investigation activities, supporting targeting, force protection, and civil order and security. Commanders should seek to integrate ATF identity activity capabilities into DOD plans and activities to support current and future operations, as appropriate.

(c) **DEA.** The DEA utilizes unique capabilities with counterparts in the international law enforcement community and PNs to locate, track, apprehend, and seize personnel, assets, and resources used to smuggle narcotics, weapons, humans, WMD, and other illicit items of interest. The DEA leverages the identity activity capabilities of the FBI, DHS, and DOD in executing its mission around the globe. In return, DOD receives valuable identity data and associated derogatory information collected from DEA objective locations for future use during military operations.

(3) **ODNI.** The mission of the ODNI is to lead the intelligence integration throughout the 17 organizations that make up the IC. The ODNI integrates intelligence analysis and collection to inform decisions made from the White House to the battlefield. The ODNI oversees two national centers that assist the conduct of identity activities.

(a) **NCTC.** NCTC is staffed by personnel from multiple departments and agencies. The NCTC is the primary organization in the USG that integrates and analyzes intelligence pertaining to terrorism and CT, including all intelligence related to terrorist use of WMD. It is the CT community lead for identifying critical intelligence problems, key knowledge gaps, and major resource constraints. NCTC co-locates intelligence, military, law enforcement, and homeland security networks to facilitate information sharing across USG departments and agencies. In addition to its information sharing role, the NCTC provides a strategic-level operational planning function for CT activities and is responsible for integrating all elements of national power toward successful implementation of the national CT strategy. As part of NCTC's mission, it maintains the TIDE, the authoritative database of all KST identifiers maintained by the USG. DOD operational intelligence components can leverage this information to support operational planning as well as tactical encounters. NCTC capabilities can also support the screening and vetting of potential intelligence sources or persons of interest to the JFC.

(b) **NMEC.** The NMEC coordinates FBI, Central Intelligence Agency, DIA, and National Security Agency efforts to exploit, analyze, and disseminate information gleaned from millions of pages of paper documents, electronic media, videotapes, audiotapes, and electronic equipment seized by the US military and IC in operational theaters around the globe. These exploitation and analysis activities can provide valuable insights into the capability, capacity, and intent of threat actors operating within the OE. NMEC products can be used by all-source and DOD law enforcement criminal intelligence analysts and investigators to inform detailed assessments and estimates to meet the commander's information and intelligence requirements. DIA serves as the executive agent (EA) for NMEC.

(4) **DHS.** DHS protects the US against threats to the homeland, secures and manages the nation's borders, protects critical infrastructure, and ensures the nation's resilience to disasters. The DHS Office of Biometric Identity Management provides biographical, biometric, and encounter data on aliens who have applied for entry, entered, or departed the US. DHS agencies, along with DOS, contribute this valuable information, which DOD leverages to enhance employment of identity activities. Entities within the DHS that contribute to identity activities include:

(a) **United States Coast Guard (USCG)**. The USCG collects identity data and related derogatory information within its role to protect US economic and security interests in maritime regions, including international waters, US coastal regions, ports, and waterways. The USCG's jurisdiction and law enforcement authorities allow it to perform operations that DOD is not permitted to perform under US law, such as maritime interdiction and other maritime law enforcement activities. USCG personnel can collect identity data and forensic and DOMEX materials anywhere in the world, with certain restrictions, in support of military operations while retaining their Title 14, United States Code (USC) authorities, even if assigned as additional Title 10, USC forces.

(b) **CBP.** The CBP works through existing partnerships with customs and law enforcement agencies in PNs to protect US borders and ports of entry, and screen the admissibility of persons, cargo, and vessels arriving into US ports. CBP maintains the National Targeting Center–Passenger and provides I2 analysis capabilities and encounter management of potential DOD threat actors who are subsequently encountered by DHS screening organizations.

(c) **Immigration and Customs Enforcement (ICE).** ICE enforces US immigration and customs regulations. One of its highest priorities is to prevent illicit procurement networks, terrorist groups, and hostile nations from illegally obtaining US military products; sensitive dual-use technology; WMD; or CBRN materials. The ICE Office of Homeland Security Investigations' Biometric Identification Transnational Migration Alert Program is an initiative that fills biometric databases with data collected from special interest aliens, violent criminals, fugitives, and confirmed or suspected terrorists encountered within illicit international pathways. This data helps I2 analysts form strategic pictures of the trends, networks, and individuals connected with these pathways. As a law enforcement organization, homeland security investigations can enhance the CCDR interactions with nonmilitary foreign entities to establish identity data sharing partnerships.

(5) **DOS.** As the lead US foreign affairs agency, DOS formulates, represents, and implements the President's foreign policy. The Secretary of State is the President's principal advisor on foreign policy and the person chiefly responsible for US representation abroad, except for CT within regions where the responsibility lies with the military commander as designated by the President. DOS has six regional bureaus that address foreign policy considerations on a regional basis. The assistant secretaries of the regional bureaus are key actors in CT, SSA, and operations policy within their assigned regions. Furthermore, the DOS Bureau of Counterterrorism acts as the principal coordinator for regional bureau issues related to proposed military engagements related to identity information sharing and identity activity partner capacity building efforts.

(a) **COM.** The COM is the personal representative of the President and the official USG representative in the host country. The COM is responsible for the conduct of relations with the host government and is the primary channel for communications with that government. The COM directs, coordinates, and supervises all USG executive branch employees in that effort, except those under the command of a US military commander. Identity activities conducted by DOD and other USG departments and agencies require COM concurrence prior to execution, unless otherwise directed by the President.

(b) **US Country Team.** All USG identity activity-related strategies, plans, programs, and initiatives that are undertaken to support an HN government are managed through the elements of the US country team. The US country team is the primary interagency coordinating structure and focal point for unified action and is composed of the senior member of each represented department or agency within the embassy. The country team is headed by the COM, who is normally the ambassador, and is responsible for integrating US efforts in support of the HN. As permanently established interagency organizations, country teams are a primary resource for CCDRs wishing to support an HN to enhance or conduct identity activities. They often provide deep reservoirs of local knowledge and interaction with the HN government and population. CCDRs should coordinate with country teams, through the SDO/DATT, early in the identity activities planning process to ensure the activities are in line with US Presidential strategy, foreign policy objectives, and the COM's published country plan.

See JP 3-08, Interorganizational Coordination During Joint Operations, *for more information on country teams.*

3. Department of Defense Organizations, Responsibilities, and Relationships

a. **OSD.** OSD develops, coordinates, and oversees the implementation and integration of DOD identity activity-related policies and programs. OSD oversees the development and implementation of identity-related capabilities, standards, and frameworks and coordinates with interagency partners for the mutual development, transition, transfer, and/or sharing of identity capabilities between the Armed Forces of the United States and other USG departments and agencies, international agencies, or other countries, as appropriate. OSD coordinates with both DOS and JS to develop international protocols, standards, arrangements, and agreements, multinational support for identity activities within named operations and, when required, HN support. OSD coordinates with partner agencies and Under Secretary of Defense organizations in support to homeland security activities and international rule of law, such as terrorist watch listing or immigrant and refugee security vetting. OSD also coordinates the integration of technical DOD processes and procedures within the USG intelligence and law enforcement communities.

(1) **The Under Secretary of Defense for Acquisition, Technology, and Logistics (USD[AT&L])** is the principal staff assistant (PSA) and advisor to SecDef on all DOD biometrics and defense forensic enterprise-related matters. USD(AT&L) oversees and directs the activities of DOD biometrics, DOD Forensic Enterprise, and the DOD EAs for those capability areas, respectively. The PSA is the primary DOD point of contact for other USG departments and agencies and international entities for all biometric and forensic-related issues and activities, unless specified otherwise by SecDef or statute.

(2) **The Under Secretary of Defense for Intelligence (USD[I])** is the PSA and advisor to SecDef on all intelligence, CI, security, and other intelligence-related matters. USD(I) exercises SecDef's authority, direction, and control over DOD agencies and DOD field activities and provides strategic oversight over all DOD intelligence, CI, and security policy, plans, and programs. USD(I) provides oversight and direction to Defense Intelligence Components regarding the application and use of I2 and the execution of

identity activities to support intelligence operations. USD(I) also provides oversight and guidance for the annual budget for the Military Intelligence Program and monitors the implementation and execution of the program to support identity activities by the Services and the heads of the CSAs.

(3) **USD(P)** is the PSA and advisor to SecDef on all matters related to the formulation of national security and defense policy and the integration and oversight of DOD policy and plans to achieve national security objectives. The USD(P) oversees the plans, programs, and conduct of defense relationships with foreign governments, their military establishments, and international organizations. CCDRs must coordinate all proposed military engagements with the appropriate USD(P) country desks as early as possible in the planning process. USD(P) has further assigned responsible officials to support specified CCMD activities:

(a) **The Assistant Secretary of Defense for Homeland Defense and Global Security (ASD[HD&GS])** is the OUSD(P) coordination focal point for all identity activity military engagement activities. ASD(HD&GS) is responsible for facilitating resolution of all CCMD issues related to identity activity foreign military engagement and international information sharing, in coordination with the Office of the USD(I), JS, DIA I2PO and DFBA.

(b) **The Director, International Security Programs** is the OUSD(P) responsible official for all identity activity-related information sharing arrangements and agreements. The Director, International Security Programs maintains the approved MOC template and is the OUSD(P) coordinating official for USD(P) approval of all non-intelligence identity information sharing arrangements and agreements.

(4) **The Under Secretary of Defense for Personnel and Readiness** is the PSA and advisor to SecDef and Deputy Secretary of Defense for total force management and oversees the Defense Manpower Data Center (DMDC). The DMDC maintains identity information on each uniformed Service member (i.e., active duty, retired, reserve), US-sponsored foreign military, DOD and uniformed services civilians, and their eligible family members. JFCs can utilize DMDC's identity information to support personnel recovery (PR) operations and NEOs and to inform physical access control decisions at foreign military installations.

(5) **DOD EAs**

(a) **Secretary of the Army (SECARMY).** SECARMY is the DOD EA for both DOD biometrics and non-digital/multimedia forensics, in accordance with Department of Defense Directive (DODD) 8521.01E, *Department of Defense Biometrics*, and DODD 5205.15E, *DOD Forensic Enterprise (DFE)*. Within these roles, SECARMY leads the requirements, architecture, and standards development efforts for joint, common, and interagency biometric and non-digital/multimedia capabilities. SECARMY has designated the Army Provost Marshal General as the responsible official for executing the assignments of the EA. Within this role, the Army Provost Marshal maintains oversight, direction, and control of two sub-components to support military operations and activities.

1. **DFBA** executes the common storage, processing, matching, and sharing activities of the DOD biometrics enterprise. DFBA operates and maintains the authoritative repository (i.e., ABIS) for biometrics collected on foreign nationals throughout the course of military operations, and shared by PNs and interagency partners. DFBA performs the dissemination of the DOD BEWL on behalf of DIA and provides the conduit for matching against interagency authoritative data sets.

2. **The Defense Forensic Science Center (DFSC)** provides full-service forensic support (criminal, expeditionary, and reachback) to Army and DOD entities worldwide. The DFSC provides the Services and CCMDs specialized forensic training and research capabilities as well as forensic support to other USG departments and agencies when appropriate. DFSC contains two primary elements. The US Army Criminal Investigation Laboratory provides traditional forensic capabilities to support worldwide criminal investigation across all military Services and acts as the EA for the DOD Convicted Offender DNA Databasing Program. The Forensic Exploitation Directorate provides expeditionary and reachback battlefield forensic capabilities to support JFC requirements, to include forensic-related identity activities. The Forensic Exploitation Directorate also provides support to exercises and training as well as CCMD partner capacity building activities.

(b) **Secretary of the Air Force (SECAF).** SECAF serves as the DOD EA for digital/multimedia forensics, including those disciplines relating to computer and electronic device forensics, audio forensics, image analysis, and video analysis. SECAF executes these responsibilities through the Defense Cyber Crime Center, which provides digital/multimedia forensics exploitation; cyberspace investigative training; research, development, test and evaluation; and cyberspace analytics for cybersecurity, critical infrastructure protection, law enforcement and CI, DOMEX, and CT activities.

(6) **CJCS.** CJCS serves as the principal military advisor to the President, NSC, and SecDef regarding DOD identity activities and apportions, assigns, or allocates identity-related capabilities to plan and execute the mission. Subject to the CJCS's authority, direction, and control, the JS coordinates with CCMDs and Services to ensure identity activities are executed in compliance with domestic, international, and foreign laws, policies, treaties, and agreements. CJCS assists with interagency support for identity activities and in planning and exercising identity activities within JPP. CJCS also coordinates and provides intelligence support to the CCDRs for human target identification and prioritization. When required after SecDef approval, the CJCS will publish appropriate execute orders for identity activities.

(a) **The JS J-2 (Intelligence)** provides continuous intelligence support, to include I2 products, to the CJCS, JS, National Military Command Center, and CCMDs in the areas of targeting, warning, and current intelligence. The JS J-2 also has the responsibility for coordinating the intelligence planning activities of the Services and intelligence CSAs in support of CCDRs. The JS J-2 represents and advocates CCMD views on I2 to the JS and OSD, coordinates with the CCMDs to staff intelligence-related CJCS orders (e.g., alert orders, planning orders, warning orders) and coordinates requests for forces in response to a CCMD request for I2 production capabilities.

(b) **The JS J-4 (Logistics)** integrates logistics planning and execution in support of joint operations to drive joint force readiness, maximize the JFC's freedom of action, and advise the commander on logistics matters to include applicable operational contract support matters. The JS J-4 coordinates with the CCMD J-2 and the applicable lead Service for contracting to ensure all locally employed persons and other contracted organizations supporting DOD activities are properly vetted as required by law and policy.

(c) **The JS J-5 (Plans)** represents the CJCS in all foreign military engagement activities planned and executed by the CCMD. JS J-5 regional and country officers provide the primary connection between the CCMD, USD(P) country desks, and relevant Service elements. The JS J-5 also acts as the military advisor to the NSC Biometrics and Identity Management IPC. CCDRs should coordinate all identity activity foreign military engagements with USD(P) through the appropriate JS J-5 country officer.

(d) **The JS J-8 (Force Structure, Resources, and Assessment)** represents the CJCS in all biometrics and forensics-related topics, issues, and activities. The JS J-8 Force Protection Division coordinates with the responsible officials of the CCMDs and Services to resolve the biometric and forensic operational issues and capability gaps of the CCDRs.

(7) **Military Departments and Services.** The Services train operational and Service intelligence personnel in identity activity TTP appropriate to their Service and mission; equip their forces with the materiel needed to conduct identity activities during tactical operations; and produce and disseminate I2 products to meet JFC and, as assigned, Defense Intelligence Analysis Program requirements. The Services execute the following responsibilities in identity activities:

(a) Organize, train, equip, and otherwise prepare military forces to conduct identity activities in support of the CCDRs.

(b) Contribute to shaping an international environment hostile to VEOs, proliferation, and transnational crime and strengthening deterrence through partner capacity building and PN information sharing relationships.

(c) Coordinate identity activity capability needs with CJCS and advocate for military capabilities to conduct identity activities.

(d) Maintain and expand identity activity technical expertise.

(e) Provide subject matter expertise to support CCMD requirements in identity activities, as directed.

(8) **CCMDs.** Geographic and functional CCMDs may conduct identity activities to enable military operations, create desired effects, and support the achievement of military objectives. Via the intelligence planning process, the CCDR, through the CCMD J-2 and supported by the JIOC, ensures the standardization of I2 products within the command and subordinate joint forces, and establishes theater procedures for collection management and the production and dissemination of I2 products.

(a) **Geographic CCMDs.** The GCC is responsible for all identity activities conducted by assigned forces operating under the authority of the CCDR. The GCC detects, deters, and prevents attacks against the US, its territories, and bases, and employs appropriate forces to defend the nation should deterrence fail. The GCC is also the single point of contact for military matters within the AOR, excluding areas within the US. GCCs direct the planning and execution of identity activities within their regional strategies and policies and they determine identity activity shortfalls, identify mission-related resourcing requirements, and incorporate identity activities into their operational, campaign, and concept plans.

1. **JIOC.** The JIOC integrates and synthesizes the multitude of inputs required to holistically characterize the OE during the JIPOE process. It also ensures its JIPOE analysis is fully integrated with all I2 and JIPOE products produced by subordinate commands and other organizations. The JIOC identifies information gaps in intelligence and identity-related databases and formulates collection requirements and RFIs to address these shortfalls. Intelligence planners plan the entirety of the integrated intelligence operation (collect, exploit, analyze, produce, and disseminate intelligence) for the JFC and the planning staff. The production requirements matrix and the J-2 staff estimate are foundations for the intelligence planning effort and the basis for federated analysis and production.

See JP 2-01.3, Joint Intelligence Preparation of the Operational Environment, *for detailed description of I2 support to the JIPOE process.*

2. **Joint Interrogation and Debriefing Center (JIDC).** A JIDC conducts follow-on exploitation of detainees and EPWs. Detainees and EPWs are screened and those of further intelligence potential are identified and forwarded to the JIDC for follow-on interrogation and debriefing in support of JTF and higher requirements. Besides detainees and EPWs, the JIDC also may debrief civilian detainees or internees, refugees, displaced persons, legal travelers, and other non-prisoner sources. Identity activities support both the screening and interviewing of these population sets, facilitating detailed foreknowledge of the interview subject and effective exploitation of those personnel during debriefing or interrogation.

See JP 3-63, Detainee Operations, *for a detailed description of biometric, forensic, and I2 support to detainee operations.*

3. **Joint Document Exploitation Center (JDEC).** A JDEC collects and exploits captured materials (e.g., documents, cell phones, and electronic media such as computer files, video) to obtain intelligence. Material exploitation can obtain information on a great range of topics, such as information on adversary intentions and planning (including deception), locations, dispositions, tactics, communications, logistics, and morale as well as a wealth of information for subsequent long-term exploitation. Exploited materials can support the identification of threat actors, the mapping of their networks, and inform capability, capacity, and impact assessments of those networks. The resulting I2 products support follow-on strategic and operational planning as applicable.

4. **Joint Personnel Recovery Center (JPRC).** The JFC may establish a JPRC or its functional equivalent. The JPRC, in coordination with any separately organized component PR coordination cells, employs identity activity capabilities to facilitate and enhance PR efforts during an isolating event. Verification of the identities of recovered personnel (whether alive, deceased, or incapable of providing information) is a critical PR consideration.

See JP 3-50, Personnel Recovery, *for details on identity activity support to PR.*

5. **KLE Cell.** A KLE cell may be established to map, track, and distribute information about the key nodes within the human environment in the JOA. The KLE cell should establish and maintain a human environment database and I2 KLE production requirement, conduct pattern analysis, develop a detailed background briefing on each key leader, suggest specific approaches for encouraging support for joint force activities/objectives, ensure debriefs are conducted following KLEs, and update the human environment map with current intelligence and debrief information. The cell provides field units and staffs an updated human environment map, background information, I2 assessment, and desired effects for KLE across the operational area.

(b) **USSOCOM.** The Commander, USSOCOM provides direct identity activities support (e.g., training, equipment, exploitation, I2 analysis) to globally deployed SOF and supported GCCs. Where appropriate, SOF identity activities and capabilities are synchronized and integrated with the identity activities and capabilities of both CF and partners in order to achieve unity of effort. The TSOC is the primary theater SOF organization to plan and control special operations and other SOF activities, including identity activities. The TSOC plans and conducts operations in support of the GCC. The TSOC is generally responsible for the planning of identity activities executed in support of SOF operations and will be the main conduit between USSOCOM and the GCC.

See JP 3-05, Special Operations, *for a detailed description of SOF I2 operations, capabilities, and activities.*

(c) **United States Cyber Command (USCYBERCOM)** is a subunified command under US Strategic Command. USCYBERCOM identifies, targets, and attributes cyberspace actions, events, or associations to individual cyber-personas. The cyber-persona layer (i.e., an individual's or group's online identity[ies]) holds important implications for joint forces in terms of positive target identification and affiliation, and activity attribution. These identification, affiliation, and attribution efforts require significant collaboration with other commands, agencies, or organizations to be effective. Because of its singular focus on CO, USCYBERCOM conducts significant identity activities and leverages the identity activities of both DOD and interagency partners' operational and intelligence components to assist its efforts to connect a cyber-persona or cyberspace action to an actual individual, group, or state actor, with sufficient confidence and verifiability to hold them accountable.

(9) **CSAs**

(a) **DIA.** DIA has oversight of the Defense Intelligence Analysis Program and is the DOD focal point for BEI and FEI as well as four intelligence disciplines (measurement and signature intelligence, HUMINT, CI, and open-source intelligence), and represents all Service and CCMD requirements for national intelligence collection in those areas. DIA analysts provide support in identity activity areas such as all-source human factors analysis, CT, counterproliferation, counterdrug operations, PR, peacekeeping, multinational support, NEO, warning intelligence, targeting, current intelligence, systems analysis of the adversary, collection management, intelligence architecture and systems support, intelligence support to operation planning, KST watch listing, and DOMEX, BEI, and FEI.

1. **The Director, DIA** is the intelligence lead for BEI and FEI and is responsible for establishing and maintaining military and military-related intelligence agreements and arrangements with foreign governments and other entities. The Director, DIA serves as the DOD BEWL Manager and the DOD nominator to the National KST Watch List and is responsible for coordinating and synchronizing the development and implementation of identity activity-related collection strategies across the Services and CCMDs.

2. **The DIA I2PO** is the defense intelligence focal point and advocate for all matters relating to I2, BEI, and FEI. The DIA I2PO provides subject matter expertise to CCDRs and staff on planning, executing, and assessing identity activities; I2 analysis and production; and partner engagement activities. The DIA I2PO develops and synchronizes identity collection planning in support of CCMD operational objectives, supports CCMD military engagement and MOC development activities, and facilitates DIA's Office of Partner Engagement (OPE) coordination and approval of I2-related sharing arrangements and agreements. The DIA I2PO also provides direction and oversight for DOD BEWL development, management, and sharing efforts on behalf of the Director, DIA.

See Department of Defense Instruction (DODI) 3300.04, Defense Biometrics Enabled Intelligence (BEI) and Forensics Enabled Intelligence (FEI), *for additional information about the DIA I2PO.*

3. **The DIA OPE** coordinates and approves the negotiation and conclusion of military and military-related intelligence agreements and arrangements between DOD components and foreign governments, international organizations, or other entities on behalf of the Director, DIA. All CCDR I2-related sharing agreements and arrangements must be coordinated and approved by DIA OPE.

4. **The Defense Combatting Terrorism Center Watch Listing Division** evaluates non-SIGINT-derived DOD reporting to nominate terrorists to the NCTC for inclusion on the National KST Watch List maintained by the Terrorist Screening Center in fulfillment of HSPDs 6, 11, and 24. This information enables federal, state, and local screening agencies to deny terrorists access to the US homeland. Complete and accurate collection of identity data and derogatory information related to individuals encountered in the operational area by tactical forces is critical to supporting these nominations.

(b) **JIDO J-2.** JIDO leads DOD actions to rapidly provide counter-improvised threat capabilities in support of CCDRs and to enable the defeat of the IED as a weapon of strategic influence. JIDO leverages identity activities to support all CCMDs in defeating the improvised devices and attacking IED and improvised weapon employment networks. The JIDO J-2 supports JIPOE development by delivering fused I2 products on threat networks that employ improvised weapons. The JIDO J-2 also tracks the global illicit and threat network connections through multiple CCMDs, countries, and continents to identify the threat actors who coordinate, supervise, and operate the critical capabilities of the networks.

See DODD 2000.19E, The Joint Improvised Explosive Device Defeat Organization, *for additional information about JIDO.*

4. Nongovernmental Organizations

NGOs are highly diverse groups of organizations conducting a wide range of activities and take different forms in different parts of the world. NGOs and military units each play essential roles in providing humanitarian assistance and disaster relief during both natural and man-made emergencies. Identity activities support military efforts to provide humanitarian assistance, to include enabling resource control activities, transportation and relocation efforts, medical support, and other activities in addition to security and force protection. The use of identity information, especially biometric data, can provide a bridge between military and NGO assistance activities. Commanders should coordinate with appropriate interagency counterparts as intermediaries and when appropriate, directly with the NGOs themselves to coordinate the collection, storage, and use of identity data during emergency assistance operations.

5. Indigenous and Surrogate Entities

a. Violent extremists, transnational criminals, and/or weapons proliferators often seek safe harbor among the civilian populace of a sovereign nation without the consent of local authorities or the national government. A PN may have the national will to apprehend or expel terrorists and/or transnational criminals from inside their borders, but lack the resources and expertise to act. Concurrently, direct US action may be counterproductive to achieving operational objectives. To mitigate these security challenges, indigenous or surrogate forces may be employed to support or conduct identity activities. These forces may resemble SOF, CF, security forces, or friendly opposition elements used during UW operations or campaigns.

b. Using USG assets to remove threat actors unilaterally on behalf of a foreign government may present diplomatic, political, and legal risks. In these circumstances, pursuing threat actors with or through regular indigenous forces or surrogates offers several advantages. They generally speak the local language, are sensitive to local culture, and have personal knowledge of the civilian populace. More importantly, they may be legally empowered by their national or local governments to conduct military or law enforcement operations within national borders. CCDRs may seek to enable indigenous or surrogate forces with identity activities capabilities with DOD reachback support. This combination allows indigenous actors to leverage the identity activity capabilities of the joint force, while

maintaining the needed level of operational distance and legitimacy. It also enables US efforts to build partner capacity and further professionalize partner forces within a strategic framework of stabilization activities.

c. Generally, SOF has the mission to train, equip, and support indigenous armed forces, police, or other internal security forces. CCDRs may also task CF to provide limited identity activity support to PN security elements, upon request of the HN. SSA biometrics, forensics, or DOMEX capacity building activities, approved by the COM, may additionally be used to support shaping and deterrence strategies. Regardless of the approach used, CCDR coordination of HN support activities will involve the US country team, and potentially a number of interagency partners as well.

6. Multinational Organizations

Multinational organizations such as INTERPOL and NATO can be key partners in the employment of effective identity activities as they also maintain and employ identity activity capabilities to support their operations and constituents. While these capabilities may be robust, commanders should seek to understand the legal, political, and cultural frameworks under which they have been established and can be employed well before US forces are deployed to ensure all the necessary agreements, arrangements, and procedures are in place to support effective collection, processing, exploitation, data sharing, storage, and use. Similarly, commanders should ensure they understand and have adequately planned for differences in the technical standards, TTP, and communications architectures required to interoperate with these strategic partners. The USG may have multiple relationships and agreements with these organizations that must be thoroughly considered and respected to avoid confusion, overlap, and the potential for unintended diplomatic/political consequences.

Intentionally Blank

CHAPTER V
SPECIAL CONSIDERATIONS

1. General

The strategic environment is characterized by uncertainty, complexity, and rapid change, which requires persistent engagement. Threats to the US are fluid, with continually shifting alliances, partnerships constantly appearing and disappearing. While it is impossible to predict precisely how challenges will emerge and what form they might take, we can expect that uncertainty, ambiguity, and surprise will dominate the course of regional and global events. In addition to traditional conflicts with peer and near competitors, significant and emerging irregular threats continue to develop, affecting the nation's ability to project power and maintain its influence and qualitative edge. Within this environment, JFCs must plan, execute, and assess identity activities under a range of legal authorities, policy constraints, transnational threats, regional concerns and biases, and most likely within a multinational operational setting.

2. Authorities

Pursuant to US and international law, DOD components have authority to collect, process, and exploit identity information, forensic materials, and captured materials. These activities, however, may be subject to limitations, restrictions, or conditions on collection and data use depending on the circumstances (time, place, manner, and purpose) of the activity. Identity activities may be conducted during times of peace or conflict; at home, abroad, or on the high seas. The collection may be obtained through a variety of means and methods, and the identity information may be used for a variety of purposes supporting operations. Additionally, in certain circumstances, a JFC may choose to apply or conform to HN law. JFCs and their staffs must be cognizant of these circumstances and assess their legal impacts (restrictions, limitations, or conditions), if any, on the operation and the identity activities conducted to support it. In each instance, commanders should seek the counsel and recommendations of their operational law SJAs to ensure the legal sufficiency of their actions.

a. **Law of War.** In accordance with DOD policy, DOD personnel comply with the law of war during all armed conflicts. However, such conflicts are characterized, and in all other military operations. See DODD 2311.01E, *DOD Law of War Program*. Identity activities must fit within the scope and authority of the mandate that authorizes the operation (e.g., Presidential directive, congressional authorization to use military force, United Nations [UN] Security Council resolution, and/or general principles of self-defense [UN Charter Article 51]). The law of war traditionally regulates the resort to armed force, specifically, the conduct of hostilities and the protection of war victims in both international and non-international conflict, belligerent occupation, and the relationships between belligerent, neutral, and non-belligerent states. It is derived from the Hague Convention, treaties, Geneva Conventions, and customary international law with the intent to protect combatants, noncombatants, and civilians from unnecessary suffering, provide certain fundamental protections for persons who fall into the hands of the enemy, facilitate restoration of peace, assist military commanders in ensuring the disciplined and efficient use of military force, and

preserve the professionalism and humanity of combatants. The protections provided by the law of war may not inhibit, limit, or restrict the routine means of conducting identity activities during periods or in places of conflict. They may, however, restrict the employment of identity activities to avoid violations of international human rights standards. For example, the taking of a facial photograph for identification is not prohibited but the use of it to degrade or humiliate a prisoner of war is prohibited under Article 13 of the Third Geneva Convention.

b. **Law of the Sea.** Within the maritime domain, the conduct of identity activities is principally challenged by the circumstances of the activity. During times of conflict or hostilities, employment of identity activities will be guided by the law of war, UN Security Council resolutions, and congressional authorizations to use force. During peace time, different laws apply depending on the physical location (e.g., internal waters, territorial waters, archipelagic waters, contiguous zones, or the high seas) where the activity is being conducted. Rules pertaining to innocent passage, transit passage, and sovereign immunity may affect collection and use. Different rules also apply depending on the types of operations being conducted (e.g., approach, visits, searches). Under these rules, certain classes of individuals (e.g., foreign naval personnel) may be specifically protected. Specific case-by-case authorizations may be required prior to conducting identity activities depending on the circumstances.

For more information, refer to Navy Tactics, Techniques, and Procedures (NTTP) 3-07.11M/Coast Guard Tactics, Techniques, and Procedures (CGTTP) 3-93.3/Marine Corps Interim Publication (MCIP) 3-33.04, Visit, Board, Search, and Seizure Operations.

c. **Geneva Conventions and UN Declarations**

(1) The four Geneva Conventions of 1949 apply as a matter of international law to all military operations that qualify as international armed conflicts and cases of partial or total occupation. These treaties are intended to provide comprehensive humanitarian standards for the treatment of war victims and detainees, and the protection of civilians without adverse distinction. Commanders must ensure the employment of identity activities complies with the Geneva Convention treaties, most notably in the treatment of EPWs and the protection of civilians in a time of war.

(2) Certain identity activities may be broadly interpreted within the UN's Universal Declaration of Human Rights as subjecting individuals to arbitrary interference with their privacy. However, it should be noted that legitimate interference is clearly permitted within international and intergovernmental law (e.g., EU law) by a state interested in enforcement of the just requirements of morality, public order, and the general welfare. As such, JFCs are traditionally authorized to obtain and use identity information for legitimate purposes as a matter of public order or general welfare, which include national security, in both international and non-international armed conflict situations.

d. **HN Law**

(1) The desire to conduct identity activities within an HN's borders during peace time (e.g., to enhance protection of overseas installations and personnel) will require compliance with HN law. Commanders should coordinate with their SJAs and the US country team to review HN law as well as pertinent agreements between DOD and the HN (e.g., defense cooperation agreements, status-of-forces agreements). The appropriate SDO/DATT should have situational awareness of all identity activities being conducted within the HN.

(2) HN law governing an individual's right to privacy could significantly affect how and what identity activities can be employed during a military operation; limiting certain uses, requiring specific handling conditions for identity information, and/or restricting the means of collection.

3. Legal and Policy Considerations

Identity activities are likely to involve a myriad of legal and policy considerations. Because of the nature and complexity of the operational legal issues involved (e.g., law of war, ROE, RUF, detainees, dislocated civilians, negotiations and involvement with local and HN governments), the SJA should be consulted early and frequently throughout identity activity planning and execution.

a. **The Privacy Act.** The Privacy Act (Title 5, USC, Section 552a) prescribes how USG departments and agencies are to maintain (defined as maintain, collect, use, or disseminate) identifying information (record) about a US person (citizen or legal permanent resident). A record is identified as any item, collection, or grouping of information about an individual to include biometric, biographical, or other identifying data. The Privacy Act does not apply to non-US persons nor non-living US persons; however, the Privacy Act does apply to combatant and noncombatant US persons. The Privacy Act generally affords an individual for whom an agency maintains information notice that the agency has the record, access to see the record, ability to consent to the sharing of the record, and ability to submit a letter of disagreement about the information maintained. Military units that encounter individuals who claim to be or are believed to be US persons may be required to provide certain notifications (e.g., Privacy Act statements) and/or specifically manage collected information in compliance with the Privacy Act. JFCs who believe they may have collected personally identifiable information on a US person or are operating in an area populated with US persons should consult their SJA for guidance on Privacy Act requirements.

b. **Leahy Vetting Requirements.** The Leahy Amendments (Section 620M of the Foreign Assistance Act of 1961) prohibit the USG from providing funds to a unit of the security forces of a foreign country if DOS has credible evidence the unit has committed gross violations of human rights. The provisions restrict funding until the Secretary of State determines and reports that the government of such country is taking effective measures to bring the responsible members of the security forces to justice. All SSA activities, and some intelligence collection operations, related to identity activities will require Leahy vetting before they are implemented.

c. **National Policy Considerations**

(1) **Executive Order (EO) 12333, *United States Intelligence Activities.*** EO 12333 regulates the use of national intelligence assets. Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers and their agents, threat organizations, and actors is essential to informed decision making in the areas of national security, national defense, and foreign relations. Collection of such information is a priority objective and should be pursued in a vigorous, innovative, and responsible manner that is consistent with the Constitution and applicable law and is respectful of the principles upon which the US was founded. JFCs collect information through identity activities concerning and conduct activities to protect against international terrorism, proliferation of WMD, foreign intelligence activities, international criminal drug activities, and other hostile activities directed against the US by foreign powers, organizations, persons, and their agents in accordance with priorities set by the President. This information must be collected, managed, shared, and used pursuant to the authorities and restrictions of the US Constitution, applicable law, the policies and procedures authorized in DODD 5240.1, *DOD Intelligence Activities*, and other relevant DOD policies authorized by USD(I). Special emphasis should be given to the protection of the constitutional rights and privacy of US persons.

See DODD 5240.1, DOD Intelligence Activities, *for more information.*

(2) **Presidential Directives**

(a) **National Security Presidential Directive (NSPD)-59/HSPD-24, *Biometrics for Identification and Screening to Enhance National Security*.** The use of biometrics improves DOD's ability to identify and screen persons for whom an articulable and reasonable basis for suspicion exists that they pose a threat to national security. The directive instructs all federal agencies to make available to other agencies biometric and associated biographical and contextual information associated with such persons. NSPD-59/HSPD-24 identifies the importance of collecting and sharing identity information across government agencies and has provided a foundation to apply biometrics technologies to the collection, storage, use, analysis, and sharing of identification data.

(b) **HSPD-6, *Integration and Use of Screening Information to Protect Against Terrorism*.** To protect against terrorism, it is the policy of the US to develop, integrate, and maintain thorough, accurate, and current information about individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism and use that information as appropriate and to the full extent permitted by law. Operational commanders shall, on an ongoing basis, collect and provide all appropriate identity information on terrorists encountered in the OE to the NCTC through the DIA Watch Listing Division.

(c) **HSPD-11, *Comprehensive Terrorist-Related Screening Procedures*.** In order to more effectively detect and interdict individuals known or reasonably suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism and terrorist activities, it is the policy of the US to enhance terrorist-related screening through comprehensive coordinated procedures that detect, identify, track, and interdict people, cargo, conveyances, and other entities and objects that pose a threat to

national security and to do so in a manner that safeguards legal rights, including freedoms, civil liberties, and information privacy guaranteed by federal law. In accordance with this directive, commanders shall conduct biometric and biographic screening using national terrorism information at all appropriate opportunities. This screening shall be conducted across the conflict continuum in support of all combat operations and every mission or activity where foreign nationals are encountered and a privilege, access, and/or benefit determination is made.

(d) **NSPD-33/HSPD-10, *Biodefense for the 21st Century*.** The US places special emphasis on the need for proactive steps to confront biological weapons threats. Consistent with this approach, DOD is focused on detecting and, when possible, destroying an adversary's biological weapons assets before they can be used. The use of identity activities further expands existing capabilities to interdict enabling personnel, technologies, and materials, including through the Proliferation Security Initiative, and enhances supporting intelligence capabilities to provide timely and accurate information to enable proactive prevention. Early detection, recognition, and warning of biological actors of concern and weapons proliferation networks permits timely responses at the tactical, operational, and strategic levels to deter their use, inhibit their movement, and mitigate the potential consequences of their activities. Deterrence is the historical cornerstone of biological weapon defense, and attribution—the identification of the perpetrator as well as the method of attack—forms its foundation. Biological weapons lend themselves to covert or clandestine attacks that permit the perpetrator to remain anonymous. Continuous use of identity activities enhances the deterrence posture by improving attribution capabilities through technical forensic analysis and I2 attribution assessments.

(e) **PPD-18, *Maritime Security Policy*.** Due to its complex nature and immense size, the maritime domain is particularly susceptible to exploitation and disruption by individuals, organizations, and states. The maritime domain facilitates a unique freedom of movement and flow of goods while allowing people, cargo, and conveyances to transit with anonymity not generally available over land or by air. Individuals and organizations hostile to the US have demonstrated a continuing desire to exploit such vulnerabilities. Under its existing authorities, DOD deploys its full range of operational assets and capabilities to prevent the maritime domain from being used by terrorists, criminals, and hostile states to commit acts of terrorism and criminal or other unlawful or hostile acts against the US, its people, economy, property, territory, allies, and friends. JFCs execute identity activities, consistent with US law, treaties and other international agreements, to enhance the security of and protect US interests in the maritime domain, including, but not limited to countering terrorist travel, conducting counter-piracy operations, interdicting illicit traffickers, and enhancing maritime domain awareness.

(f) **PPD-23, *Security Sector Assistance (SSA)*.** The US shares security responsibilities with other nations and groups to help address security challenges in their countries and regions, whether fighting together in a multinational environment; countering terrorist or international criminal networks; participating in international peacekeeping operations; or building institutions capable of maintaining security, law and order, and applying justice. Multiple actors contribute to SSA, but unity of effort across the USG is essential. For this purpose, the US applies a whole-of-government approach to planning,

synchronizing, and implementing SSA to ensure alignment of resources and national security priorities. This approach applies to identity activity military engagement activities. CCDRs seeking to provide PNs with identity activity-related articles, training, or services should consult the Defense Security Cooperation Agency and seek DOS review and approval as required.

See JP 3-20, Security Cooperation, *and the* Defense Security Cooperation Agency Security Assistance Management Manual, *for more information.*

(3) **Intelligence Community Directives (ICDs)**

(a) **ICD 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*.** DNI has established guidelines that address mandates in the *Intelligence Reform and Terrorism Prevention Act of 2004* to strengthen the sharing, integration, and management of information within the IC, and established policies for discovery and dissemination or retrieval of intelligence and intelligence-related information collected or analysis produced by the IC. The overall objectives of this policy are to foster an enduring culture of responsible sharing and collaboration within an integrated IC; provide an improved capacity to warn of and disrupt threats to the US homeland, US persons, and US interests; and provide more accurate, timely, and insightful analysis to inform decision making by the President, senior military commanders, national security advisors, and other executive branch officials. To this end, JFCs shall treat identity information collected and I2 analysis produced as national assets and, as such, shall act as information stewards who have a predominant responsibility to provide. In addition, authorized IC personnel have a responsibility to discover identity information and I2 believed to have the potential to contribute to their assigned mission need and a corresponding responsibility to request the relevant identity information and I2 they have discovered. Commanders are responsible for the proper handling and use of information received from a steward. All discovery, dissemination, retrieval, and use of identity information or I2 collected, analyzed, or produced shall be consistent with applicable law and in a manner that fully protects the privacy rights and civil liberties of all US persons, as required by the Constitution, US law, EOs, Presidential directives, court orders, and Attorney General-approved guidelines, including those regarding the dissemination of US person information, and consistent with the *Guidelines to Implement Information Privacy Rights and Other Legal Protections in the Development and Use of the Information Sharing Environment*.

(b) **ICD 302, *Document and Media Exploitation*.** DOMEX is the processing, translation, analysis, and dissemination of collected hard copy documents and electronic media, which are under the USG's physical control. DOMEX is a core component of identity activities, providing critical insight into the capability, capacity, and intent of threat actors and networks. DOMEX serves to illuminate behavior, patterns of life, associations, and the potential level of knowledge and expertise of threat actors encountered in the OE. Acknowledging the importance of DOMEX activities and capabilities, the DNI has established the NMEC to advance the IC's collective DOMEX capabilities and ensure prompt and responsive DOMEX support to the JFC and subordinate elements.

(c) **ICD 304, *Human Intelligence*.** DNI policy addresses clandestine and overt HUMINT collection obtained both inside and outside the US to integrate, prioritize, and maximize the IC's HUMINT capabilities; ensure coordination and deconfliction of HUMINT and CI operations and activities across the USG; and enable greater collaboration across the USG to share services of common concern wherever feasible. ICD 304, *Human Intelligence,* delineates the roles and responsibilities of the DNI, the National HUMINT Manager, and those principal agencies of departments that execute HUMINT, CI, or other activities. JFCs may choose to conduct identity activities using both clandestine and overt HUMINT means. This type of employment should be coordinated and deconflicted comprehensively and continuously at the lowest practicable level, typically through the embassy station chief. JFCs may provide training and equipment to PN personnel to enable them to collect intelligence and CI information in response to DOD and/or national intelligence requirements. These activities are conducted for the primary purpose of collecting intelligence and not for the purpose of building partner capability and capacity. Operations and activities conducted for these purposes are coordinated and deconflicted with the relevant embassy COMs and ODNI through the appropriate chiefs of station, according to standard IC policies and practices. All DOD training, export control, and other relevant issues are processed in accordance with Defense Security Cooperation Agency Manual 5105.38-M, *Security Assistance Management Manual,* as required.

d. **NDP.** NDP governs the disclosure of US classified military information to foreign governments and international organizations. While identity information is normally unclassified, certain conditions (e.g., method or source of collection) can cause the information to be classified confidential or above. Similarly, most I2 is classified according to derivative classification rules established in Department of Defense Manual (DODM) 5200.1, *DOD Information Security Program,* Volumes 1-4. However, certain I2 products (e.g., subsets of the DOD BEWL) can be promulgated at the unclassified/for official use only level. Identity information and I2 is useful only when it is provided to those who can act on it, and in many cases that includes foreign allies and PNs. For this reason, identity activity-related information and I2 products should be developed and maintained in a manner that facilitates the broadest degree of responsible sharing whenever possible.

e. **DOD Policy Considerations**

(1) **DOD Issuances**

(a) DODD 8521.0E, *Department of Defense Biometrics,* establishes policy and assigns responsibilities for DOD biometrics. The DOD biometrics enterprise provides a critical end-to-end capability through a defined operations-intelligence cycle to support tactical and operational decision making across the conflict continuum for DOD warfighting, intelligence, law enforcement, security, force protection, HD, CT, business, and information environment mission areas. The DOD biometric and intelligence enterprises are integrated and interoperable through the use of I2 capabilities, including BEI, to the fullest extent possible to enable DOD and mission partners' operations. SECARMY is designated as the DOD EA for biometrics and leads and executes common storage, matching, analysis, and sharing activities of the DOD biometrics enterprise for biometric data collected as a part of military operations.

(b) DODD 5205.15E, *DOD Forensic Enterprise (DFE),* establishes policy and assigns responsibilities within DOD to develop and maintain an enduring, holistic, global forensic capability to support the full conflict continuum. The DOD Forensic Enterprise consists of those DOD resources, assets, and processes that provide forensic science analysis linking persons, places, things, and events. The directive designates the SECARMY as the DOD EA for those forensic disciplines relating to DNA, serology, firearms and tool marks, latent prints, questioned documents, drug chemistry, and trace materials, as well as forensics relating to forensic medicine disciplines such as forensic pathology, forensic anthropology, forensic toxicology, and DNA analysis to identify human remains. It further designates the SECAF as the DOD EA for digital/multimedia for those forensics disciplines relating to computer and electronic device forensics, audio forensics, image analysis, and video analysis.

(c) DODD 3300.03, *DOD Document and Media Exploitation (DOMEX),* establishes policy, assigns responsibilities, and provides direction for DOD DOMEX in accordance with DODD 5105.21, *Defense Intelligence Agency (DIA),* and ICD 302, *Document and Media Exploitation*. The processes for collection, analysis, and dissemination of DOD DOMEX-derived information shall be integrated into military operational planning and execution at all levels; use standardized methods of collecting and processing documents and media captured or otherwise acquired during DOD operations; focus on rapid and broad dissemination of both raw data and finished exploitation products to tactical, operational, strategic, and national customers; and utilize the NMEC as the central DOD clearinghouse for processing DOD-collected documents and media.

(d) DODD 5240.1, *DOD Intelligence Activities,* and DOD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons,* set forth the conditions under which DOD can conduct intelligence activities, including when DOD intelligence assets may collect and retain information on US persons. Within the limits of the law, DOD may collect and retain information on US persons reasonably believed to be engaged in foreign intelligence or terrorist activities, among other reasons set forth in Procedure 2 of DOD 5240.1-R. Because of the numerous legal restrictions placed on the collection of intelligence against US persons, all intelligence activities must be coordinated with the servicing SJA before execution.

(e) DOD 5400.11-R, *Department of Defense Privacy Program,* provides guidance on section 552a of Title 5 USC, the Privacy Act of 1974, as amended, and prescribes uniform procedures for implementation of the DOD Privacy Program.

(f) DODD 5200.27, *Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense,* establishes general policy, limitations, procedures, and operational guidance pertaining to the collection, processing, storage, and dissemination of information concerning persons and organizations not affiliated with the DOD. This directive prohibits collecting, reporting, processing, or storing identity information on individuals or organizations not affiliated with the DOD, except in those limited circumstances where such information is essential to the accomplishment of DOD missions. Several core DOD identity activity capabilities have been granted an exception to this policy.

(g) DODI O-3300.04, *Defense Biometric Enabled Intelligence (BEI) and Forensic Enabled Intelligence (FEI),* establishes DOD policy and assigns responsibilities for management and execution of BEI and FEI and support to I2 activities. Additionally, it establishes the I2PO within DIA to coordinate and synchronize BEI and FEI activities. Effective BEI and FEI are an integral part of the DOD biometric and forensic enterprises and are strategically important identity activity intelligence processes used to unambiguously identify persons, networks, and populations of interest who pose potential threats to US forces and national security.

(2) **OSD Memorandums.** In accordance with OSD memorandums, the CCDRs and the Military Departments are authorized to employ DOD biometric capabilities in concert with our PNs in order to meet the full range of mission requirements, as permitted by law. The use of international partnerships for biometric information collection in various manners, including leading and/or assisting in biometric collection efforts in PNs and acquiring information from a PN under a sharing agreement is authorized. The categories of non-US persons from which biometric information can be collected, stored, enrolled, shared, and analyzed are:

(a) Persons encountered during maritime interception/interdiction operations.

(b) Persons detained under the law of war or pursuant to military operations.

(c) Persons of interest.

(d) Local employees.

(e) Third-country nationals.

(f) Non-US persons seeking access to DOD facilities and installations.

4. Transnational and Regional Considerations

US security interests will continue to be threatened by increasingly complex and volatile irregular threats with transnational tendencies. These threats will attempt to elude US capabilities by concealing themselves in dense urban populations and by dispersing their operations through cyberspace. Transnational threats may include one or a combination of terrorists, insurgents, opposing factions, and organized criminal elements. Controlling or containing their proliferation is particularly difficult due to the growing number of weak or failing states, ungoverned spaces, and the globalization of crime. These actors are lured by large profits gained through illegal enterprises and the power to influence relevant populations toward those ends. Many threat networks have resorted to criminal sourcing to fund themselves to offset or replace dwindling state-sponsorship. Decreased state-sponsorship, combined with globalization and information systems, have allowed these groups to grow more autonomous. CCDRs should pay particular attention to synchronizing and integrating the activities of assigned, attached, and supporting forces to achieve national, theater, and/or multinational strategic objectives. Due to the transnational nature of various enemies or adversaries (e.g., insurgents, terrorists, drug cartels, pirates), coordination and synchronization requirements may also extend to adjacent GCCs. CCDRs and subordinate

JFCs must work through a myriad of sociocultural factors and issues, while simultaneously operating within the political constraints of a MNF to be successful.

a. **Presence of Other Relevant Actors in the OE**

(1) **Other State Actors.** Regional state actors can be pivotal to the dynamics and outcomes of a joint operation. If supporting the adversary, they can provide critical access to sanctuary areas and resupply as well as a scale and scope of resources otherwise typically unavailable to non-state armed groups. Conversely, regional state actors allied with the joint force can coordinate the control of borders, cut adversary logistic networks, interdict illicit activities, and counter the exploitation of border areas as sanctuaries. The use of identity activities is essential to disrupting the flow of foreign fighters in and out of the theater of operations. Enabling regional state actors to screen and interdict transnational criminals, violent extremists, and opportunities attempting to evade the reach of the friendly force can be a critical step in breaking the enemy's ability to effectively conduct operations and achieving military objectives.

(2) **Transnational Criminal Actors and Networks.** Population density and complex physical terrain allow criminals to blend into the population. Some discount organized criminal groups as a national security or military threat. However, a band of criminals without any political ideology could use the same methods as more traditional threats for profit and cause significant disruptions to security, stability, and US national interests. Sometimes these syndicates may have better resources than insurgents. The percentage of a population that involves itself in organized criminal behavior need not be great to present a threat to stability. A criminal group that can control one district of a 10-million plus megacity has more power than most rural insurgents could gain over 20 years of operations. Such power will need to be addressed by any intervening force.

(3) **VEOs.** Transnational political movements that use unlawful violence to advance their objectives are referred to as VEOs and are de facto terrorists. VEOs may initially start as adherents of a localized or transnational political movement, bound together by ethnicity, religious belief, caste affiliation, or common goal. While these groups tend to be motivated by real or imagined unjust treatment from a government (or governments), these VEOs may turn to transnational organized crime to provide financial, material, or personnel support, despite a purported abhorrence for criminal or immoral activity.

b. **Sociocultural Considerations.** The social variable unquestionably affects the execution of military operations within the OE. Indigenous populations are typically subject to the same political authority, occupy a common territory, have a common culture, and often share a sense of identity. Each significant concentration of people has its own demographic characteristics: population density, neighborhoods and their make-up, ethnicity, race, age, daily movement, and other considerations based on the nature and behavior of the populace. Other socio-cultural characteristics may include religion, political leanings and activity, economics, clan or tribal affiliation, criminal organizations and activities, and class divisions. Understanding cultural, political, social, economic, and religious factors, both local and regional, is often central to mission success and the population should be considered as a distinct and critical aspect of the OE. The local and regional populations are

an obvious and required focus of identity activities but that focus may adversely affect the achievement of strategic and operational objectives depending on the cultural, religious, and political elements that form the social fabric of those societies. Commanders should view indigenous populations as sources of information but also critical components of post-combat success during stabilization and transference activities. When conducting identity activities, commanders should keep in mind the traditional objectives regarding civilians: to minimize civilian interference with military operations; minimize mission impact on the population; and observe the necessary legal, moral, and humanitarian obligations toward civilians.

(1) **Social Structure.** Social structure refers to the relations among groups of persons within a society and involves the arrangement of the parts that constitute society, organization of social positions, and distribution of people within those positions. Understanding social structure provides insight into how a society functions and informs collection and analysis efforts. Races and ethnic groups are key aspects of social structure because they are often key sources of friction within an OE. Religious groups may be subsets of larger ethnic groups. I2 analysts must understand the dynamic interaction among groups within the social structure, to include formal relationships (e.g., treaties, alliances), informal relationships (e.g., customs, common understanding), divisions or cleavages, and cross-cutting ties (e.g., religious alignments that cut across ethnic differences) as well as the importance of roles, status, and norms within the society.

(2) **Cultural Issues.** Culture is a system of shared beliefs, values, customs, behaviors, and artifacts that members of a society use to cope with their world and with one another. Culture is habitual and perceived as "natural" by people within the society. Culture conditions an individual's range of action and ideas; influences how people behave and make judgments about what is right, wrong, important, or unimportant; and dictates how members of a society are likely to perceive and adapt to changing circumstances. Whereas social structure comprises the relationships within a society, culture provides meaning. Identity activities often require direct contact and interaction with the local population and cultural understanding is a key to their successful execution. The cultural tendencies of the local population may be very different from what friendly forces are accustomed to and should be considered when establishing the ROE for collection of identity information and use of identity activity capabilities among the local population. Personal grooming habits, living conditions, laws, customs, and social beliefs and superstitions can significantly affect the warfighter's ability to conduct identity activities as well as the quality of the products they produce for the commander. The sensitivity and finesse with which friendly forces navigate these cultural tendencies during the execution of identity activities can play a pivotal role in maintaining the legitimacy of the operation as a whole.

c. **Political Instability.** Political instability can be described as the condition, process, and consequences of stress in a sovereign state or other governing system stemming from the system's inability or refusal to satisfy the political, social, economic, religious, or security wants and needs of its population. It often stems from or leads to a loss of authority or control over persons, territory, or interests. Politically unstable states and ungoverned spaces generate local and regional conflict and humanitarian crises. These areas are vulnerable to exploitation by other states and transnational groups. Various regional state actors and/or

transnational networks may exploit voids left by politically unstable governments to conduct illicit activities or expand their sphere of influence. Weak or nonfunctioning states may be unwilling or incapable of defending their basic sovereignty or of performing even basic government functions in contested areas. Additionally, religious, ethnic, and tribal conflicts are common sources of friction that foster patronage and corruption and undermine nation-states, ultimately, further undermining the legitimacy of the host government.

d. **Regional Treaties and Alliances**

(1) **EU.** The EU maintains strict protections for personal privacy and data protection that affects the legal authority of EU nations to collect and maintain identity data. In some instances, an EU partner can collect identity information in a foreign theater of war as long as it is disposed of at the end of military operations. In other instances, the partner can collect and maintain data but cannot share it if there is a potential that information will be used to detain or otherwise interfere with an individual's basic human right to privacy. In all instances, the national law of EU partners will define how, when, and for what purpose identity information can be collected, stored, used, and shared. However, certain exemptions typically exist to facilitate the legitimate use of identity information to support national security, military, and law enforcement activities.

(2) **NATO.** The ability of NATO's members to conduct identity activities is subject to each member's national laws and policies. CCDRs are encouraged to leverage the framework NATO has developed to manage the complexities of collecting and sharing identity information between members. The NATO Biometrics Programme Coordination Group coordinates all matters related to the use of biometric technologies in support of NATO operations and develops required capabilities to support nations collecting and sharing biometric data in support of NATO operations. NATO is also initiating similar coordinating and institutionalization efforts for I2 and human network analysis and targeting. CCDRs are also encouraged to consult NATO's framework policy, technical standard (i.e., NATO Standardization Agreement 4715, *NATO Biometrics Data, Interchange, Watchlisting and Reporting),* and doctrine (i.e., Allied Intelligence Publication-15, *Countering Threat Anonymity: Biometrics in Support of NATO Operations and Intelligence),* which provide guidance on the use of biometrics under NATO operations.

5. Multinational Operations

US commanders should expect to conduct identity activities as part of a MNF conducting military operations. These operations, which could occur in a formal multinational alliance or a less formal coalition, could span the conflict continuum and require coordination with a variety of other interorganizational partners. To effectively employ identity activities, commanders and staffs must be cognizant of differences in partners' laws, doctrine, organization, equipment, terminology, culture, politics, religion, and language, and partner to craft appropriate solutions to achieve unity of effort. Multinational considerations also include international law, agreements, arrangements, and national laws and caveats required to protect the sovereign interests of troop-contributing countries.

a. Whenever possible, identity activities should include participation by the HN and multinational partners. Multinational partners may possess robust collection, processing, exploitation, and intelligence resources, or at least niche capabilities that may provide invaluable access and insight regarding particular aspects of the OE. Many of these countries may also have extensive regional expertise based on their historical experience.

b. When conducting identity activities that involve interaction with nonmilitary organizations, it is important to consider the ramifications of labeling identity information or releasable I2 products as intelligence. In many cultures, the perception of intelligence connotes information gathered on an HN citizenry for coercive purposes. Furthermore, attempts to exchange information with many NGOs and IGOs may prove difficult. Most NGOs and IGOs are eager to maintain political neutrality and are unlikely to associate with any overt or perceived intelligence gathering attempts. Nevertheless, identity information and I2 product exchange throughout the operational area for the purposes of fostering mutual interests in resolving or deterring conflict or increasing security is highly beneficial to all concerned parties. Information exchange should comply with US and DOD security guidelines.

c. For operations, the responsibility and authority for using military force is generally delegated from the President through SecDef to the supported CCDR/JFC in the form of approved plans/orders with either ROE for operations overseas or RUF. When compared to major combat operations, ROE for some smaller-scale operations (i.e., some CT operations) may be more restrictive and detailed, especially in an urban environment, due to national policy concerns for the impact on civilians, their culture, values, and infrastructure. A JFC may begin operations with different ROE/RUF for each type of mission or activity, which may affect his rules for employment of identity activities. When conducting identity activities, the JFC responsible should determine early in the planning stage what the required rules of employment should be, including anticipating the need for changes based on changing conditions, evolution in the phases of an operation, and branches/sequels to a plan. Depending upon the required level of approval, that JFC must take anticipatory action if the changes are to be timely enough for effective operations. When conducting identity activities in a multinational environment, the use of identity activity capabilities may be influenced by the differences between US and HN or PN ROE/RUF. Commanders at all levels should consult with their SJA and take proactive steps to ensure the individual Service member understands the current ROE because a single errant act could cause significant adverse diplomatic/political consequences.

d. The joint force will typically operate in a complex international environment alongside other actors that will have a need for identity information and I2 products. They are also likely to possess valuable information they can provide the joint force that is unique to their own mission and sources. The sharing of identity information, while often unclassified, requires careful control and assessment, continuously weighing the benefits of sharing against the possible risks of data compromise and the potential for unintended use of US-provided information. Concurrently, the data provided by a PN, if false or inaccurate, may have far-reaching and strategic impacts on a broad variety of national security activities. The JTF J-2 and or CCMD J-2 must have a process in place to responsibly exchange information with external sources and assess the validity of information supplied by mission

partners. This process should include FDOs with sufficient training and experience in sharing identity information and the proper authority to disclose classified I2 products to foreign governments and international organizations in accordance with legal and policy guidelines. Mission partners may include USG interagency members, UN organizations, PNs, allied military and security members, local indigenous military and security forces, NGOs, and private companies and individuals providing contract services within the operational area. Although the joint force may have organic identity activity capabilities assigned, these mission partners may provide the bulk of collection, processing, and exploitation capabilities.

e. A multinational identity activities effort requires interoperable data and data exchange capabilities. Whenever possible, participants should agree to work from a standard collection and transmission specification to facilitate interoperable processing and exploitation. A multinational identity activities plan should address how all data will be shared between member forces, including disclosure and release procedures for I2 information and products. The CCDR should work to standardize data schemas, operating procedures, and TTP prior to the need to deploy to a combat zone and regularly test these arrangements during multinational exercises. This construct will allow PNs to effectively institutionalize these factors into their traditional training, doctrine, and employment mechanisms. DOD has established approved data and transmission standards for multiple capabilities that enable identity activities. It has also ratified biometric standards and BEI reporting formats within the NATO policy. All of these approved standards are based upon current published national standards.

APPENDIX A
IDENTITY ACTIVITIES SUPPORT TO OPERATIONAL MISSIONS

1. Introduction

a. Identity activities support and enhance a significant amount of offensive, defensive, and stability operations and activities. Identity activities play an especially critical role in any OE where there are dynamic populations of civilians, criminals, opportunists, facilitators, terrorists, and irregular forces. Within this complex environment, the ability to identify, characterize, and effectively manage the identities of enemies, adversaries, and persons of interest alike becomes essential to mission success. Whether conducting military engagement, security cooperation, crisis response, limited contingency operations or major operations and campaigns, forces will conduct identity activities to accomplish their mission objectives.

b. Below are several examples of typical mission sets that leverage identity activity capabilities to achieve military objectives. This list is not all inclusive, but demonstrates the value of identity activities across the range of military operations.

2. Support to Alien Migrant Interdiction Operations

Alien migrant interdiction operations are as much humanitarian missions as they are law enforcement. The USCG is the lead agency for the enforcement of US immigration laws at sea. The USCG patrols and coordinates with a multitude of federal, state, and local agencies, as well as foreign countries, to interdict illegal migrants at sea.

a. Currently, the USCG conducts biometric screening on both migrants and those who smuggle them in the Mona Pass off the coasts of South Florida and Puerto Rico. Biometric and biographical information is collected in an attempt to positively identify each individual.

b. This information is submitted to and screened against the DHS IDENT where it is enrolled and retained for future identification. If there is a derogatory match within IDENT on the migrant or smuggler, that information is sent to the appropriate sector command center.

c. Simultaneously, biographical information obtained from the migrant and/or smugglers is transmitted to the USCG maritime intelligence detachment to initiate development of an I2 report for each migrant. An established regional concurrence team provides a disposition for any matched or unmatched persons for follow-on action.

d. In some cases, the matched migrants are turned over to local border patrol authorities for processing and/or prosecution. Watch listed and warranted individuals are turned over to local authorities for prosecution on outstanding offenses. All other persons onboard are returned to the Dominican Republic in accordance with existing bilateral agreements.

3. Base Access and Entry Control Points

a. Identity activities are a powerful force protection tool and joint forces should employ identity capabilities in base access and entry control point (ECP) missions for US-controlled facilities.

b. ECPs provide controlled access to specific areas, canalize traffic, or positively identify those who are passing thorough a given area. They are also frequently used to support other operations, such as to screen employees; control facility, warehouse, or storage access; and protect defense critical infrastructures. Identity activities support checkpoint operations by positively identifying those passing through the checkpoint. Biometrically enabled access cards, used in conjunction with a regular screening process at the ECP, protect our forces and those of our PNs by positively identifying the bearer of the access card. ECP planning considerations:

(1) Fully enroll all personnel who are allowed regular access to an installation and issue them a biometrically enabled access card. Regardless of past efforts, do not assume this has been done.

(2) Biometrically screen all personnel entering or leaving your base even if they possess an access card. A biometrics handheld collection device does this very quickly.

(3) Plan and establish checkpoints for verification.

(4) Canalize all traffic to checkpoints.

(5) Use “overwatch” to spot individuals trying to avoid checkpoints.

(6) Ensure up-to-date BEWL, for the unit’s operational area, is uploaded to the handheld collection devices for verification.

PERSONNEL SCREENING AND VETTING FOR INSTALLATION ACCESS

The new installation Commander at Kandahar Airbase has determined the need to fully enroll and verify the identity of all locally employed personnel (LEP) working on the installation. It is estimated this operation must support the screening of 1,600 personnel.

The local contract team checks the personal identification of each LEP and performs a full biometric enrollment. The security team checks each enrollment against the latest biometric-enabled watch list before submitting it to the Department of Defense authoritative database for matching. Full biometric enrollments of individuals include fingerprints, iris images, facial images, plus biographical information and the contextual data related to the collection event. All enrollment information is retained in recurrent vetting purposes and to support future employment verification activities.

Various Sources

(7) Plan for full electronic biometric transmission specification enrollments of suspect individuals.

4. Border Control/Ports of Entry/Maritime Interception/Checkpoints

a. Biometrics is extremely effective for managing and tracking cross-border movements. Checkpoints provide an effective means to stop the flow of foreign fighters and seal off the JFC's area of interest. Our enemies may find sanctuary across a border, but identity activities that include biometric data collection makes the task of returning an extraordinarily risky venture.

b. Identity activities immediately create complex terrain for the enemy by limiting the corridors they can use to access an operational area. Tracking personnel at ports of entry and border crossings produces a great wealth of information on their movements. Repeated crossings show a pattern of behavior that reveals a number of things, from migration patterns to supply routes. Simply identifying the routes of merchants and ships identifies a significant pattern.

5. Support to Site Exploitation

a. Site exploitation operations involve highly trained team members who have specific duties during the operation but should also be trained in other member's responsibilities so they can supplement the mission if something happens to a team member. Regardless of whether conducting a deliberate or hasty operation, prior planning is the key to success. Information collected is used for a variety of future missions but two important aspects of site exploitation are to properly record and preserve the evidence for future prosecutions.

b. Exploitation (forensic, technical, and mechanical) of physical materials is accomplished through a combination of forward-deployed and reachback resources to support the commander's operational requirements. The exact mix of exploitation resources will depend on the threats identified by JIPOE, the JFC's mission, and the resources available from PNs. In an IW environment, commanders are concerned with identifying the members of and systematically targeting the threat network, addressing threats to force protection, denying threat actors access to resources, and supporting the rule of law. Information derived from identity activity exploitation can provide specific information and actionable intelligence to address these concerns. Identity activity exploitation capabilities employ a wide array of enabling capabilities and resources, from forward-deployed experts to small cells or teams providing scientific or technical support, interagency or partner laboratories, and centers of excellence providing real time support via reachback. These exploitation capabilities can be employed individually to provide targeted support to distinct missions and/or functions, or together in a modular format under a common C2 construct.

(1) Site exploitation teams are specifically detailed and trained to conduct systematic search and discovery operations and properly identify, document, and preserve the point of collection and its material.

(2) EOD personnel have special training and equipment to render explosive ordnance safe, make intelligence reports on such ordnance, and supervise its safe removal.

EOD personnel exploit an incident site, providing post-blast investigation expertise and site exploitation support, including a tactical characterization of the incident and a technical categorization of the device.

(3) Weapons intelligence teams are task organized teams that exploit a site of intelligence value by collecting weapons technical intelligence-related materials, performing tactical questioning, collecting forensic materials, preserving and documenting DOMEX, providing in-depth documentation of the site, evaluating the effects of threat weapons systems, and preparing material for evacuation.

(4) When WMD or hazardous chemical precursors may be present, CBRN response teams can be detailed to supervise the site exploitation. CBRN response team personnel are trained to properly recognize, preserve, neutralize, and collect hazardous chemical, explosive, or drug-related materials. The teams have an integrated EOD capability to enhance CBRN activities and mitigate threats.

(5) In a maritime environment, US Navy surface combatants and Marine Corps units employ visit, board, search, and seizure (VBSS) teams for detecting chemical, biological, and radiological materials; collecting biometric and biographical information; conducting tactical questioning; and preserving and documenting captured enemy documents and media, including cellphones and contextual and electronic data for DOMEX. Marine Corps and Navy VBSS teams can be augmented by intelligence exploitation teams to facilitate HUMINT and tactical site exploitation activities. Where IEDs or explosive hazards are likely, EOD and combined explosives exploitation cell (CEXC) platoons can be assigned to support the VBSS missions.

(6) The US Marine Corps and USSOCOM maintain deployable exploitation analysis centers to support forensic exploitation requirements around the globe. Each exploitation analysis center provides a forensic capability with the necessary equipment and trained personnel to execute select forensic exploitation activities in an expeditionary environment.

(7) The US Army also maintains and deploys forensic exploitation teams (FXTs) when requested by a CCMD or JTF. FXTs provide an expeditionary forensic exploitation capability, including latent print examiners, DNA examiners, forensic chemists, firearms/tool mark examiners, electronic engineers, DOMEX personnel and support personnel from a modular pool, task-organized to meet mission requirements. An FXT can also be deployed modularly with other Service exploitation capabilities. FXTs support I2 and DOD law enforcement criminal intelligence analysis and production at all echelons, although their primary customers are tactical and operational commanders.

(8) CEXCs are a Naval Surface Warfare Center, EOD Technology Division deployable capability that is scalable in skills and size, allowing them to be tailored to meet the commander's requirements, including incorporation of multinational and interagency partners. CEXC personnel are trained and equipped to conduct technical intelligence operations involving recovered improvised weapons systems and provide near-real-time intelligence on their construction and employment. CEXC processes support identity

activities by identifying IED trends and bomb makers, providing insights into enemy tactics, and assisting in the development of defensive and offensive C-IED and other improvised weapons defeat measures. CEXC supports I2 and DOD law enforcement criminal intelligence analysis and production at all echelons, although its primary customers are tactical and operational commanders.

(9) The FBI's TEDAC serves as the single interagency organization to receive, fully analyze, exploit, and provide a repository for all terrorist IEDs of interest to the US. TEDAC coordinates efforts of the entire government, including law enforcement, intelligence, and military, to gather and share intelligence about these devices. TEDAC provides direct support to broader USG efforts to prevent and mitigate IED attacks by performing advanced exploitation of IEDs through physical examination, resulting in scientific and technical information and valuable intelligence. Through its integration of intelligence resources, TEDAC also provides expeditious reporting of raw and finished intelligence to intelligence and law enforcement partners about device attributes and terrorist TTP to enhance knowledge and understanding of current and future threats.

DELIBERATE OPERATIONS

Detection. Recent human intelligence (HUMINT) reporting has indicated that a mid-level terrorist leader frequents the home of the village elder following Friday prayer. This home has been previously reported to multinational forces as a terrorist safe house. Further reporting indicates that he meets with a local terrorist cell leader here. The dossier on the village elder indicates that he has eight family members who live at this home and that he is employed as a metal fabricator.

Locate/Identify. Imagery from an unmanned aerial system (UAS) and from walking patrols of the village elder's home are collected and analyzed. Images of persons detected are matched against known locals who have provided identification as well as been previously enrolled in a biometrics handheld collection device. Biometric facial matching indicates that there is a high possibility that two local farmers also attend these meetings. The UAS reveals that the home is a three building compound surrounded by an 8-foot wall. A white truck arrived first carrying three military-aged males (MAMs) with assault rifles. A small blue sedan arrived at this location shortly after Friday prayer with two MAMs, both entered the home. UAS imagery indicated that the village elder's family left the main house and went to the rear quarters. The meeting lasted for one hour and ten minutes. A forensic collector with a walking patrol arrived two hours later and recovers a water bottle and three cigarette butts from the vicinity where the white truck had parked. Latent fingerprints from the water bottle and DNA [deoxyribonucleic acid] from the cigarette butts match a biometric enrollment from two former detainees who were released six months ago. They were suspected low level terrorists who were detained on weapon charges.

Target Nomination. A target folder is developed on the house, and the persons of interest: the village elder, the two unknown persons who entered

the home, two local farmers, the two former detainees, and the unknown person with the white truck. Biometric dossiers are added to the targeting folder.

Preparation. All of the available biometric dossiers of the persons of interest are uploaded into two portable handheld biometric collection devices along with the current biometric watch list and biometric dossiers of the villagers. The first device will be carried by the initial assault team. The second device will be carried by the follow-on security force containing the multi-function team. To minimize risk to civilians, it is determined to strike the house five minutes after the arrival of the blue sedan giving time for the family members to exit the main building. The threat security force in the white truck along with the house would be hit simultaneously. All persons in and around the house will be biometrically enrolled and matched before being released.

Execution. The initial assault resulted in the capture of nine MAMs and the killing of two of the MAMs with the white truck. All were asked to show any identification documents as well as enrolled/matched with suitable biometric collection devices. Five of the eleven were previously enrolled and this aided the initial tactical questioning. The security team arrives minutes after the compound is secure and occupants are segregated. The multifunctional team begins gathering documents and computers, the HUMINT collectors begin the initial interrogation.

Imagery of the compound and all known pertinent data has been given to the planners for use in planning a successful site exploitation mission. All historic and habitual activities and social relationships are studied by the team to try and forecast all situations that might be present upon arrival of the team. A targeting mission has been planned by special operations forces to capture or kill insurgent members if encountered on this location. The site exploitation team has been put on alert that as soon as the initial mission has concluded the team will be transported to the location by helicopter to exploit any and all useful artifacts or paperwork for future intelligence value or prosecution efforts.

HASTY OPERATIONS

The site exploitation team, currently deployed to forward operating base Jasmin in the Helmand Province, has been training on proper procedures for collecting data in various scenarios. Several scenarios have been developed by the operations staff that seem to categorize most missions that the site exploitation team would need to be able to accomplish. One mission involves possible improvised explosive device (IED) makers being targeted and when the team arrives they find various devices used for making IEDs along with several MAMs that appear to be associated but not previously targeted by allied forces. Other scenarios depict failed targeting attempts because the Level 1 target sought was not at the location. Evidence at the scene however led the leadership to deploy the site exploitation team because a very high level al Qa'ida leader was presumed to frequent the residence.

The team is currently being deployed to an embassy where multiple fatalities have occurred and one of those was a very high ranking member of the Afghan government. Explosive ordinance disposal (EOD) members have cleared the area for the site exploitation team. Team members are hurried to the location where they begin sifting through the wreckage and litter. Members find pieces of the bomb that was reportedly triggered by a cellular phone and believed to be delivered by a suicidal insurgent. Shards from the bomb are carefully tagged, recorded, and transported to a laboratory located in the area. Chain-of-custody is carefully adhered to and, if fingerprints are found on the shards, they will be sent to various databases to determine whether a match can be made with an already-collected fingerprint. Once the fingerprints are matched and a high-value individual is added to the biometrics-enabled watch list, soldiers can focus on finding and prosecuting the individual responsible for murder and terroristic activities.

Various Sources

6. Support to Census Operations

The employment of biometric technologies and robust information systems makes large scale biometric supported census operations feasible and practical. Census planning considerations:

a. Locate and identify every resident.

b. Visit and record every house and business.

c. At a minimum, fully biometrically enroll all military-age males with full sets of fingerprints, full face photo, iris images, and names, including all variants.

d. Record biographical data, including addresses, occupation, tribal name, and military grid reference of enrollment.

1st Battalion is used as the example counterinsurgent force. This time Bravo Company is assisting the local municipal government in clearing overgrown irrigation canals. Bravo Company is supporting the effort by supervising the letting of a contract through the Commander's Emergency Reconstruction Program. Bravo Company provides the funds for the labor force and the local government learns to prioritize projects based on the essential service needs of the population. As part of the recruitment drive to obtain one hundred young males to provide manual labor for the canal-clearing project, Bravo Company personnel working with the local government and host nation security forces, collect the normal census and identification data, as well as biometric identity information from the young men. Of the prospective applicants, it is determined that 125 are residents of 1st Battalion's area of operations and 25 are non-residents. The prospect of a job induces the local population to commute or in some cases migrate. The Bravo Company Intelligence Support Team, working with the 1st Battalion S-2 and S-5 (Civil/Military Operations) Sections, determine the residency status by comparing the recruits' identity data to previously collected census results. The purpose of the project was not only to clear canals and build legitimacy of the municipal government, but also to win the recruiting battle with the insurgent organization by employing young men from the local area. Thus, once vetted for security concerns, Bravo Company offers employment to one hundred of the young men through the municipal public works office. Planning considerations include:

- **Locate and identify every resident;**
- **Visit and record every house and business.**
- **At a minimum, fully biometrically enroll all military-age males as follows:**
  - **Full sets of fingerprints;**
  - **Full face photo;**
  - **Iris images;**
  - **Names and all variants of names;**
  - **Record the following biographic data elements;**
  - **Address;**
  - **Occupation;**
  - **Tribal name;**
  - **Military grid reference of enrollment.**

Lessons:

- **Have staging areas and standard operating procedures for collection operations.**
- **Maintain security at all times and ensure there are personnel search teams at the entry control point for the operation. If necessary, ensure your personnel search teams include females in order to search females. Create an enrollment event for future data mining.**
- **Put residents in a common database.**

- **Collect and assess civil-military operations data.**
- **Identify local leaders and use them to identify the populace.**
- **Use badges to identify local leaders, and key personnel.**
- **Push indigenous forces into the lead at every possible opportunity.**
- **Track persons of interest; unusual travel patterns may indicate unusual activities.**

Various Sources

7. Support to Civil Affairs

a. Identity activities serve as invaluable tools for establishing or reestablishing the legitimacy of local authorities in activities that build or restore the PN's capability and capacity. The focus of such operations is to improve PN capability and capacity to provide public services to its population, thereby enhancing legitimacy of the PN, enhancing force protection, and accomplishing the JFC's objectives. Support to CA missions should emphasize long-term developmental programs that are sustainable by the HN. Use of biometrics-enabled identity management tools to manage refugee movement and relocation efforts can expedite such operations while increasing security. A unit's ability to leverage identity tools results in the means to rapidly reunite separated families. Accurately identifying families receiving aid (e.g., medical care, food, water, material, jobs) through the use of biometric signatures, controls distribution and helps to eliminate waste and black marketeering. Small units may frequently find themselves tasked to conduct or support CA operations before, during, and after combat operations.

b. CA planning considerations may include:

(1) Identify key actors in the OE.

(2) Plan for implementation of population control measures.

(3) In conjunction with the SJA, ensure that biometric enrollments do not violate any international laws or policies.

8. Support to Cordon Operations

a. In order to find selected personnel or material, a unit will typically conduct a "cordon and search" or "cordon and knock" operation. There are two primary elements in a cordon and search operation, the cordon element and the search element. Both of those elements have requirements for the collection of identity information. The search team may use several approaches to the search itself, including central assembly and restriction to quarters or control of the heads of households. In each of these approaches, biometrics can be used effectively. The cordon element can also set up check points in which biometric collection devices are used to screen individuals seeking to enter or leave the cordon area.

b. Cordon operations planning considerations.

(1) Plan for collecting identity data to include biometrics in the operation order and/or fragmentary order.

(2) Plan to conduct biometric enrollments and screening.

(3) Ensure current watch lists and local alerts are loaded before mission execution.

(4) Ensure unit and/or patrol with handheld collection devices has taken enough extra charged batteries for completion of the mission.

(5) Use biometric handheld collection devices at checkpoints in the cordon to canalize traffic.

(6) Plan for positive or negative identification of personnel.

(7) Incorporate identity data into debriefs.

(8) Enroll everyone, to include all wounded in action and killed in action.

(9) Plan for forensic data collection, to include latent fingerprints from materials, documents and media (e.g., pocket litter, found documents, found computers and cell phones).

9. Support to Counterinsurgency

a. Identifying the population in a particular area is essential to effective COIN operations. A unit needs to know who lives where, who does what, who belongs, and who does not in their operational area. While the actual term may be problematic, population management efforts are often seen as supportive of the local government, particularly if accompanied with a program that provides badges to authorized personnel which highlights the government's presence in an area. Local and tribal leaders, clan heads, and provincial governments use identity data to secure their populace against outsiders who arrive for the purpose of intimidation or other negative activities. Simply knowing who belongs in a village or area automatically spotlights those who do not. These operations also lend authority to local leadership by helping them keep unwanted individuals out of their areas and giving them the means to effectively protect their own people.

b. Every person who lives within an operational area should be identified and fully biometrically enrolled with facial photos, iris images, and fingerprints of all ten fingers (if present); along with their biographical data to include name, place of birth, scars, marks, tattoos, and other identifying information. This identity information should be coupled with other biographic data, such as where he/she lives, what they do, to which tribe, clan, village or town they belong, etc. In this manner, a unit will more easily identify outsiders or newcomers. Identity information is also useful in the transfer of authority to another unit. A unit inheriting a current census becomes much more effective in a much shorter timeframe. Population management actions also have the effect of building good relationships and rapport, since the crafted message is that the census is intended to protect them from the influence of outsiders and will give them a chance to more easily identify troublemakers in

their midst. Population management operations offer excellent opportunities to locate and identify every resident and to track persons of interest. Unusual travel patterns of individuals may indicate unusual activities.

c. COIN planning considerations.

(1) Visit and record every house and business.

(2) At a minimum, fully biometrically enroll all military age males with full sets of fingerprints, full face photos, iris images, names, and all variants.

(3) Create an enrollment event for future data mining.

(4) Put residents in a common database.

(5) Collect and assess civil-military operations data.

(6) Identify local leaders and use them to assist in identifying the populace.

(7) Use a badge system to identify local leaders, key personnel, etc.

(8) Report potential HUMINT sources to the local J-2.

(9) Designate indigenous forces as the lead at every possible opportunity for identity activities.

(10) Intelligence sections should designate specific NAIs to support identity collection activities on specified persons of interest.

10. Support to Detainee Operations

a. During the conduct of modern military operations, members of the Armed Forces of the United States must be prepared to detain a wide array of individuals. Some of these detained persons (hereafter referred to as detainees) will result from international armed conflict and will fall into the conventional category of EPW. Other categories of detainees, however, will likely result from military operations that are not typically considered international armed conflict (e.g., FHA, PO, NEOs) or may result from their particular conduct or status of the detainee (i.e., unprivileged enemy, retained personnel, civilian internee).

b. Personnel detained for any reason should be completely biometrically enrolled as quickly as possible following initial detention. Personnel detained for one reason may be found to have several other reasons for a unit to continue detaining them. Biometric matches may also provide the linkage between an individual and an event that may provide the justification for civilian trial and internment. At a minimum, it provides a tracking tool for every individual detained for whatever reason across the country. It also provides a highly effective interrogation tool in that the interrogator has more positive knowledge of a subject's movements.

c. The collection of identity data provides specific information that may be of great use in interrogation of EPWs, enemy combatants, or other suspects. Identity data may also identify detainees who are not on the BEWL. Some of these detainees may be released. Depending upon available information, and/or intelligence, detainees may also be nominated to the BEWL if it is warranted. When integrated into the overall detainee tracking and management process, biometric data verifies and supports the decision to release or transfer an individual. Biometric data enables the tracking and management of detainees within detention facilities to include departure and arrival times at various internal detention facility services. Commanders must ensure unit procedures do not conflict with HN laws on civil rights or other regional and local policies and agreements.

d. Identity activities enhance a unit's ability to:

(1) Positively identify detainees.

(2) Confirm involvement in illegal or criminal activities.

(3) Track details of interactions with detainees throughout the detention process to include release (prevent the release of the wrong person).

(4) Avoid identification mismatches due to changing and/or multiple versions of names.

(5) Individualizes personnel, i.e., regardless of how many individuals with the same name there are in the world, each one has a unique set of biometrics that differentiates them.

(6) Prepare for effective interrogation by checking the BEWL and other activities.

(7) Assist HN prosecution of individuals through identity data matches.

For more information, refer to JP 3-63, Detainee Operations, *and DODD 2310.01E,* The Department of Defense Detainee Program.

11. Support to Foreign Internal Defense

The Armed Forces of the United States regularly train the forces of PNs and regional allies. US forces are dependent on the PN to verify that those receiving our training and the benefit of our expertise are, in fact, the individuals that the PN (and the US) want to train and not adversaries. By using the simple expedient to verify the identities of individuals receiving the training (especially through the use of biometrics), and vet, the individual trained, we reduce the likelihood of training our present or future enemies. Advising the PN on the use of identity activities for such verification provides yet another means of contact with PN authorities and an avenue for further education on the usefulness of identity capabilities (such as biometrics). Using identity data to vet those personnel receiving training assists US forces to identify those who should not receive training. It also identifies those personnel whose documented conduct might be a cause for concern.

US and multinational forces are supporting a foreign state's rebuilding process, which is being undermined by smuggling into the state. The host government has only allowed US forces to use collected biometric data within the host nation. Therefore, all biometric operations are conducted using local un-trusted sources (i.e., the data is not stored in the trusted Department of Defense authoritative database).

In accordance with standard operating procedures, a truck driver provides his identity data and biometric samples to the border police at a remote international border crossing supported by US military personnel. The biometric samples and contextual information are transmitted to the local un-trusted source and subsequently compared to locally stored biometric files. The truck driver's biometric data does not match any file at the local un-trusted source and a negative response is provided back to the border police. The truck driver also is checked against local and national criminal records. The border police review the driver's provided identification, match result, associated information and other available situational information and clear the truck driver to continue. The biometric file is enrolled and stored at the local un-trusted source, as well as shared with US forces, multinational partners, and nongovernmental organizations operating within the country.

Several months later, the host nation's national police, supported by a US Government department or agency, conduct a raid on a drug smuggler's safe house and seize numerous documents and other evidence. Forensically collected latent fingerprints are compared to the local database. A match is made between the samples collected during the raid and the truck driver's previous biometric file on file. An analysis of the raid, as well as additional associated information, is completed and the truck driver's non-biometric reference information is updated with these new samples, identified for future matches, and shared with all local sources within the country.

Several days later, the truck driver attempts to cross at a different border checkpoint. He submits his individual identification and a biometric sample for verification. The sample is compared against the truck driver's biometric sample on file, which alerts the border police to the data stored at the local un-trusted source. The truck driver is detained for questioning and his biometric file is updated with the newly collected biometric sample and contextual data.

Various Sources

12. Support to Foreign Humanitarian Assistance

a. Identity data can play a critical role in FHA operations even if the HN does not have an automated identity data collection enrollment protocol or database. Humanitarian assistance and other logistical support can be provided for a number of reasons, both natural and man-made. The distribution of such aid, however, should be carefully controlled to ensure everyone gets their proper allotment without anyone being able to stockpile or hoard relief supplies. A simple "biometrics signature" provides a way to track who has or has not

received aid. The employment of identity activities both ensures there will be sufficient supplies of aid and that no one unfairly benefits from FHA operations to the detriment of the population that requires the aid (and, of course, ensures we do not inadvertently deliver aid to criminal elements and other adversaries). It should also prevent availability of relief supplies on the black market, which is inimical to both our interests and those of the HN. Biometrics can be used to enroll all recipients of humanitarian assistance to ensure there is no "double dipping" into humanitarian assistance resources. Biometrics as a receipt verification protocol can dramatically limit black marketeering or other fraudulent receipt of relief supplies. Tracking those to whom assistance has been provided is easily verified through fingerprints or iris images. In the same manner that humanitarian assistance may be controlled by the use of biometrics to prevent profiteering, medical and dental assistance benefits likewise from the same function.

b. FHA planning considerations.

(1) Biometrically enroll all recipients of humanitarian assistance to ensure no "double dipping" into humanitarian assistance resources.

(2) Using DNA testing, reunite families after a disaster.

(3) Ensure we do not provide aid to anyone on the BEWL or who has had a latent print recovered from a site of anti-MNF activities.

DISASTER RELIEF

The USG is responding to a request from a country that has experienced a catastrophic disaster. The disaster has created the immediate need to locate, rescue, and manage the affected population. The host government approves the multinational response force to collect biometric samples from the civilian population to assist with disaster relief efforts with the stipulation that the biometric information only is used to identify individuals located and rescued and to manage the flow of casualties and the displaced population; and the biometric information not be removed from the country.

Biometric data is collected as the affected individuals are rescued, treated, or entered into the refugee management process. Joint force personnel utilize the collected biometric files stored in the local un-trusted source as the reference set against which subsequent matches are made. As personnel are placed aboard transportation, provided medical and/or dental care or basic services at a disaster relief site, the individuals' biometrics are the "tokens" that authorize their access. In each instance, once the biometric file is matched, the identity is referenced against repositories of non-biometric information such as camp rosters, medical records, records of service provided, transportation logs, etc. to enable better management of services provided and needs of the population. This data and the collected biometrics are shared with the host nation and multinational partners to assist in integrating their relief efforts with those of US forces. The host

nation also compares the collected information with whatever repositories of non-biometric data may have survived the disaster (e.g., tax records, census data, voting records, individual identification records) to assist in the speedy location and reunion of families. At the request of relief organizations, the national government shares the identity data and identification results with nongovernmental organizations and neighboring countries affected by the refugee flow.

FOREIGN HUMANITARIAN ASSISTANCE—RELIEF MISSION

The US military is responding as part of an international disaster relief effort. Thousands of injured are being treated and awaiting further treatment as soon as field medical hospitals are assembled and operational. All individuals who receive medical attention within the disaster area are immediately enrolled in a Department of Defense biometric local un-trusted source that has been established for management of the refugees. All treatment records are linked to their respective biometric files. Many of the injured, after being initially treated, voluntarily relocate within the disaster area. This movement is making it difficult for medical personnel to efficiently provide medical services or track patients for follow-up treatment.

US Navy corpsmen are performing triage for refugees arriving by buses at one of the newly established US field hospitals. The corpsmen collect biometric samples from each refugee for identification purposes as part of the initial medical assessment process. The biometric files are then sent for matching against the local un-trusted source to assist with the identification of the individual and retrieve any available treatment history.

A refugee who cannot be matched against the local un-trusted source is enrolled as a new biometric file. All subsequent medical treatment will later be linked to that file. When a refugee is positively matched against the local un-trusted source, links to his medical history are accessed and his prior treatment records are retrieved. Subsequent treatment is updated in the refugee's medical record so that information can be accessed by others again in the future through utilizing the established net-centric links between the non-biometric repository (medical files), his identification documents, and his biometric file. The corpsman uses these records to aid in triage.

FOREIGN HUMANITARIAN ASSISTANCE—SECURITY MISSION

The US and multinational partners operate from several dozen military bases in an allied nation and contract locally for a wide range of services, such as: vehicle rental and maintenance, civil construction, provisioning of food and water, and waste removal. Identity data, to include biometrics data, are collected to support a wide range of activities, from base access to monitoring all contracting activities. All biometric data are matched against the local trusted source and repositories of associated information for the purposes of vetting. All samples reveal a negative match and are enrolled in the local-trusted source and further transmitted to the authoritative source.

A contracting officer encounters a dishonest local contractor who is awarded contracts and receives partial payment but never finishes the work, essentially disappearing with the money. This associated information is reported to the intelligence directorate contractor vetting cell which analyzes with relevant identity and biometric data. This analysis is transmitted to the authoritative source, the individual's biometric file is identified, and repositories of associated information are updated to include putting the vendor on the "do not contract with" list, thus barring the vendor from receiving future contracts. This information is then shared with local-trusted sources and other interested parties.

The dishonest local contractor relocates to another region and applies for new US and multinational force contracts using a different company name and false personal data. Because the personnel identification requirement was in the contract, his identification documents and collected biometric sample positively match revealing the associated information indicating his previous activities and status. As a result, the dishonest contractor's bids are eliminated. The dishonest contractor's identification and biometric files are updated with the newly collected identity data, and the attempt is shared with all appropriate authorities.

A newly arrived disbursing officer is ordered into the local community to pay a contractor for recently completed work. This officer has never met the local national to whom he is to pay a large sum of cash. Following the directions provided by a local interpreter, the disbursing officer arrives at what he believes is the office of the intended contractor. Unbeknownst to the disbursing officer, he has arrived at a fake contractor's office. As a condition of payment the supposed contractor provides his biometric information. A field match test reveals the presented biometric samples do not match the biometric file of the individual identified in the contract. The disbursing officer refuses to pay despite the local interpreter's and contractor's insistence.

Upon returning to base the disbursing officer provides the collected biometric information and his incident report to the provost marshal for investigation with the local police. The local interpreter is immediately detained on-base for questioning. The fraudulent contractor's biometric file is enrolled and stored within the local-trusted database, transmitted to the authoritative Department of Defense database, and shared with interested parties. Upon conclusion of the investigation, the provost marshal concludes that the contractor is a fraud. US military contracting offices operating within the region as well as the host nation update their respective repositories with this information.

Various Sources

13. Medical and Dental Care

a. In the same manner that FHA may be controlled by the use of identity activities to prevent profiteering, so too medical and dental assistance lends itself to the same type of control. Collecting identity data can help prevent black marketeering of medical and dental supplies and "double dipping" into such aid through the use of identity vetting and "biometric signatures" to sign for the supplies. However, with medical assistance, it can have an even more positive impact by ensuring someone does not receive the same inoculation twice or gets more medication than they are due. Many people in rural areas do not understand why the medications they receive work so well and often have the philosophy, "If some is good, more is better." There is also the potential for "doctor shopping", whereby one patient sees multiple doctors to get extra medication (especially) narcotics that will be sold later.

b. Identity and biometric data allows positive control of the distribution of medical and dental assistance and ensures that no one receives more than they should. US forces use biometric data, as well, for the tracking of records and care of its own forces. Medical aid is often well received regardless of politics. US aid providers should explain the need to create a record for adult individuals as part of the medical services. Handheld biometric collection devices blend in well in a medical environment especially since they measure physical traits. Medical civil action project and dental civil action project missions already incorporate cultural considerations and gender issues and provide a non-hostile collection atmosphere superior to a combat patrol or even a KLE. Populations will then see identity data and biometric information collection as benign and associate its use with positive results.

c. Medical and dental care planning considerations.

(1) Biometrically enroll all recipients of medical and dental assistance to ensure no "double dipping" into medical and dental resources.

(2) Medical and dental care is available to all; however, some may receive it while en route to or in a detention facility.

(3) Track personnel throughout the medical care system, in evacuation channels or in hospitals.

(4) Visits to local hospitals and clinics can also be a great way to screen the local populace and increase enrollments into a database.

14. Personnel Screening and Vetting

a. US forces use a number of locally hired personnel in deployed areas for a variety of reasons. Local hires are essential to the effective operation of forward operating bases and can be found on virtually every installation operated by US forces. The use of identity data collection (to include biometric data) enables the screening and vetting of those locally employed personnel. This includes the vetting of local security forces that receive training by US to ensure they are not members or supporters of an insurgency, criminal elements, or

other adversaries. The vetting of local leaders in deployed areas, especially during phases IV and V, assures the populace that their leaders are not adversaries or criminal.

b. Planning considerations for personnel screening and vetting.

(1) Biometrically enroll all local nationals and third-country nationals directly accompanying the force, requiring access to a military controlled facility, or working on a USG-funded project.

(2) Biometrically enroll all local national company representatives who will receive direct USG payments and selected management personnel as deemed necessary.

(3) Biometrically enroll all local personnel receiving military training.

(4) Periodically verify the identities of the workforce.

(5) Coordinate with joint force headquarters operational contract support staff and supporting contracting office to ensure contracts require biometrics validation to receive payment.

15. Support to Civil Control and Management

a. DOD support to various operations may require managing cross-boundary movement of HN civilians or managing aid and support distribution. These tasks can be streamlined and monitored through the implementation of identity screenings at various control points. Civil management efforts are often seen as supportive of the local government, particularly if accompanied with a badge and/or a credentialing program that highlights the government's presence in an area.

The Task Force Raider civil affairs team will oversee the contracting of locally based companies to construct a new school in Sarpuzen village, Dand District, Kandahar Province. The civil affairs team will vet all local national personnel to insure they are not associated with the Taliban or criminal activity. The civil affairs team has a 28-member construction team plus four company management personnel biometrically enrolled at Camp Nathan Smith.

The screening team will have biometric handheld collection devices with an updated Afghan biometrics-enabled watch list (BEWL). Due to limited Internet availability and Nonsecure Internet Protocol Router Network bandwidth, biometric data submissions will utilize the SECRET Internet Protocol Router Network. The screening team must determine if any of the host nation's personnel are matched against the BEWL and must know if these individuals' biometrically match against any existing automated biometric identification system records or unsolved latent fingerprints that indicate insurgent or criminal activity.

Various Sources

b. Planning considerations for civil security and civil control.

(1) Plan for identity data collection in the operation order/fragmentary orders.

(2) Plan for full biometrics enrollments.

(3) Plan, and establish, checkpoints for identity verification.

(4) Ensure current biometrics watch lists are loaded before the mission.

(5) Plan for all electronic biometric transmission specification submissions to be sent to the DOD authoritative repository.

(6) Ensure authorized personnel receive badges and/or credentials after vetting their identification.

(7) Establish a village database to effectively assess individual access and placement.

16. Support to Targeting

a. Targeting is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. These targeting actions imply both lethal and nonlethal effects. Successful HVI targeting operations require identity activities data exploitation and other multidisciplined intelligence. Commanders must synchronize intelligence, maneuver elements (to include SOF), fire

Due to numerous improvised explosive device attacks along Highway 1 and several caches discovered, 2nd Battalion (BN)/Task Force (TF) Raider will conduct a population management mission to identify and manage the population of Pir-E-Paymal village, Arghandab district, Kandahar province.

Every adult or adolescent male who lives within the village (population of 1,200) is identified. Additionally, they are fully biometrically enrolled with facial photos, iris images, and all ten fingerprints (if present). This information is coupled with good biographical (name, notations of scars, marks and tattoos, where they live, what they do, and to which tribe or clan they belong) and contextual data (such as the context of the encounter). In this manner, a unit can easily identify outsiders or newcomers.

2nd BN has biometric handheld collection devices and will require a modified Afghanistan biometrics-enabled watch list (Level 1 and 2 for Afghanistan plus all other levels for Kandahar Province) and they will utilize tactical radio communications with TF Raider headquarters in Kandahar City. 2nd BN also wants to submit all their biometric enrollments to the DOD authoritative database to complete the identification process for the village and require a match.

Various Sources

support systems, and others (as necessary) to engage the correct HVI target at the correct time. Accurate identity and attribution is crucial when targeting individuals hidden amongst the population.

b. Identifying the specific HVI from the rest of the populace is crucial. Identity activities that include biometrics, forensics, exploitation, and multidisciplined intelligence and operational enablers enhance the ability of the commander to conduct rapid, successful targeting operations, and assist in determining what systems will be required to complete the operation.

c. Commanders follow a targeting process to provide an agile force with enough accurate and timely information, so as to allow them to interdict, kill, capture, recover, observe, engage or substitute personnel, materiel or information. Identity activities support this process as part of a multidisciplinary effort. Targeting methodology allows for identity-focused targeting and the full capability of technical exploitation to be realized and applied. Identity activities provide specific targeting requirements that refine the actions to be completed when engaging HVIs.

d. Planning considerations for targeting.

(1) Plan for identity activity data collection in the operation order and/or fragmentary order.

(2) Plan for full biometrics enrollments and verification process.

(3) Ensure current biometrics watch lists are loaded before the mission.

(4) Use biometrics to verify target(s).

(5) Identify other potential target(s).

17. Support to Stability Operations

a. Identity activities enable numerous missions related to stability operations, including but not limited to: enforcement of sanctions; counter piracy operations; counterproliferation operations; highly accurate human environment mapping; preventing human trafficking; effective administration of FHA; and prevention of black marketeering and diversion of supplies for hoarding through the use of positive identity data and biometric signatures to sign for relief supplies. Identity activity data allows a commander to empower his counterparts in the national security forces by providing positive identification and vetting of their forces. This allows a commander to ensure that his forces have not been infiltrated by the enemy and adds to the legitimacy of his forces by increasing confidence among the populace that they are truly national forces and not personnel masquerading as such. Identity activity capabilities also assist in the identification of criminal elements, insurgents, and other adversaries.

b. Support to stabilization planning considerations.

(1) Biometrically enroll, screen, and vet all local police, army, and security forces.

(2) Use identity activities (to include biometric data collection) as a means to work more closely with HN forces (help your counterparts to be successful by culling undesirables from their ranks).

(3) Inform commanders about the true background of some of their personnel (an HN policeman might prove less effective as a policeman if he has previously been banned from an American base for stealing or is identified as belonging to an adversarial group that intends to kill or injure PN personnel within the HN police or armed forces).

While on patrol, a squad of Marines detects an improvised explosive device (IED). Explosive ordnance disposal technicians render the device safe, a forensics team manages to collect latent fingerprints and deoxyribonucleic acid (DNA) samples, and the IED components are sent to a forward forensic facility for more analysis.

The latent fingerprints are formatted into a standardized electronic file, compared to samples on file and stored locally. There is no match at the local-trusted database source and the data is enrolled into a biometric file for further processing and comparison. Both the electronic fingerprint file and DNA samples are transmitted to their respective authoritative databases for further comparison. Acknowledgement of receipt is transmitted back to the local source. Matching at the authoritative data repositories does not yield a DNA match and the sample is stored for further comparison. The biometric samples are shared with partner nations (PNs), revealing a fingerprint match to a suspected bomb maker. Based on this identification, the PN provides a facial photograph of the suspected bomb maker as well as other intelligence derived from captured documents and other sources.

Analysis of the identity data, biometrics, contextual, and associated information indicates that the suspect's last know location is outside of the joint area of operations in a third country providing sanctuary. This analysis, as well as the photograph provided by multinational partners, is sent to the Department of Defense biometric authoritative repository to update the biometric file. An alert (prompt) containing links to information located in non-biometric reference data is disseminated to tactical users to facilitate future data comparisons on their local biometrics systems should they encounter the individual.

A series of raids on suspected insurgent locations provides more identity data and biometric samples that are matched to the suspected bomb maker. This match information, the biometric files and the associated information from the previous analysis that led to his being tied to the IED incidents are shared with interested parties for further analysis. Analysis of associated information indicates that the suspected bomb maker is moving within the area of responsibility and provides locations he will likely move to. Cameras are positioned around those locations (now an identity named area of interest) and provide photographs that identify the suspected bomb maker using facial recognition. Once the suspected bomb maker is located, a tactical unit conducts a raid to apprehend him.

The raid force encounters six men at the site, all with authentic-looking local government identification in their possession. Pictures of the bomb maker provided to the raid force are outdated and do not closely resemble any individual at the raid site. However, there is a biometric fingerprint match to the suspected bomb maker. Analysis of that biometric match result and associated information from the previous analysis that tied him to the IED incident enable the raid force leader to decide to detain the individual. The other men are released after collecting their biometric samples and comparing them against available repositories to determine if they had been encountered previously. All collected samples and contextual information are updated in their respective biometric files and annotated to reflect that the raid force encountered them in the company of a known bomb maker. Other information found at the scene is also collected by the raid force and subsequently stored in a repository of associated information for use in later analysis.

Various Sources

18. Support to Logistics

Identity activities allow commanders to control and manage the distribution of property to HN personnel. Requirement of a biometric signature, such as fingerprints, from those receiving supplies of any sort prevent those same supplies from diversion, hoarding, and resale. While adding to the overall identity databases, it also ensures that payments are made to the correct person by verifying that person's identity. The US forces frequently use locally employed personnel in the conduct of logistical and transportation operations. The biometric enrollment and vetting of locally employed personnel, as required by the Federal Information Processing Standard Publication 201-2, Personal Identity *Verification of Federal Employees and Contractors,* mitigates the hiring of adversaries and criminal elements.

19. Support to Countering Weapons of Mass Destruction

Identity activities can be valuable in countering WMD. International cooperation on precursors and essential components, supplemented by identity activities data, can prevent the proliferation of such weapons, identifying personnel associated with various storage sites and involved in their trafficking. Forensics is particularly effective in sorting the wheat from

the chaff: personnel apprehended on site with WMD can be positively linked to the weapon by matching latent fingerprints and DNA found on key components or in key locations to the biometric records of personnel, separating innocent personnel from those who had intimate access to the weapons themselves. Forensic exploitation of WMD can also provide valuable information as to the source of supply of critical components and yield detailed information about supply chains, allowing more effective response and interdiction possibilities.

20. Support to Chemical, Biological, Radiological, and Nuclear Response

Biometrics allows the JFC to closely control access to CBRN-affected areas and to physically control access to residents and authorized personnel only. Simple iris image technology can give the commander the ability to decide who can or cannot enter a particular area. In a CBRN incident, this ability offers clear operational advantages. By scanning the irises of all legal residents and authorized personnel and placing them in a simple database, commanders create the ability to control access to any cordoned area. Forensic processing of the scene is simpler, containment is easier, and future medical treatment, if needed, will go to those actually affected, reducing incidents of attempted medical fraud.

21. Support to Counter Threat Finance

Forensic techniques are key factors when it comes to tracking financial transactions and financial activities. Criminal and insurgent activities are dependent on adequate funding. The forensic exploitation of digital media, computer hard drives, cell phone histories, and subscriber identity module cards provides the tools needed to track the history of financial transactions from the end user back to the source, allowing US forces to identify both personnel and opportunities to interdict funding of illicit activities. Using forensic techniques to trace financial records and identify financiers also allows the JFC to reinforce the rule of law and individual sovereignty of PNs. The use of identity data is also used to track finance records for friendly forces.

Intentionally Blank

APPENDIX B
IDENTITY INTELLIGENCE SPECIALIZED PRODUCTS

1. Overview

I2 is the intelligence resulting from the processing of identity attributes concerning individuals, groups, networks, or populations of interest. I2 fuses identity attributes (biographical, biological, behavioral, and reputational information related to individuals) and other information and intelligence associated with those attributes to identify and assess threat actors and networks, their capabilities and capacity, centers of gravity, objectives, intent, and potential COAs in support of the commander's decision-making process. The JFC receives current identity information and derogatory reporting from all levels of the joint force (including operational, intelligence, and law enforcement elements), the IC, interagency partners, and PNs concerning KSTs, foreign fighters, foreign intelligence agents, criminals, opportunists, actors of concern, and persons of interest. The intelligence generated through all-source analysis of identity activities can take several forms; ranging from graphic displays to traditional reports, disseminated from UNCLASSIFIED to TOP SECRET security protocols; in support of a wide variety of military operations and activities. The following discussion illustrates some specialized I2 products currently in use. Additional products tailored to specific situations may be devised by local I2-trained all-source analysts, limited only by their intelligence, imagination, and creativity.

2. Department of Defense Biometrics-Enabled Watch List

The DOD BEWL is a list of persons of interest in which individuals are identified primarily by their biometric sample instead of their name or other biographical information. This DOD-wide service managed by the National Ground Intelligence Center, serves as the tool that gets the critical conclusions about threat identities from BEI out to the field. This watch list can be customized depending on mission, and disseminated at the unclassified/for official use only level. The BEWL is shared with interagency partners to enhance the effectiveness of their screening operations, and can be shared with international partners, on a case-by-case basis, after completing a foreign disclosure review.

3. Biometric Intelligence Analysis Report

A biometric intelligence analysis report is a 2-3 page assessment focused on an individual actor, derived from one or more biometric match prompts that fuses all-source intelligence with biometric information to assess and characterize observed behavior and assess the level of potential threat.

4. Identity Intelligence Tracking Intelligence Package

An identity intelligence tracking intelligence package (I2TIP) is a multi-intelligence product that provides tailored summaries of significant derogatory information on individual persons of interest and their known movements in an easily briefed format. These products enhance understanding of where threat actors have been known to operate, their known associates, and insights into their potential capabilities to support tracking and targeting

activities. I2TIPs enable improved force protection, targeting operations, enhanced intelligence collection, and coordinated operation planning in a multinational environment. A sample I2TIP is depicted in Figure B-1.

5. Visual Intelligence Product

A visual intelligence product is primarily a graphic assessment that provides brief summaries of key persons and networks of interest to support operation planning and targeting. Visual intelligence products are generally produced for senior leaders and policy makers.

6. Tactical Visual Intelligence Product

A tactical visual intelligence product is an all-source intelligence graphic product that fuses BEWL encounters, matches to IEDs, I2 and network information, and other geospatial layers to highlight ideal geographic locations to conduct cordon and search operations, tactical biometric collection operations, support targeting activities, and HN law enforcement actions.

Sample Pre-Operation Identity Intelligence Tracking Intelligence Package

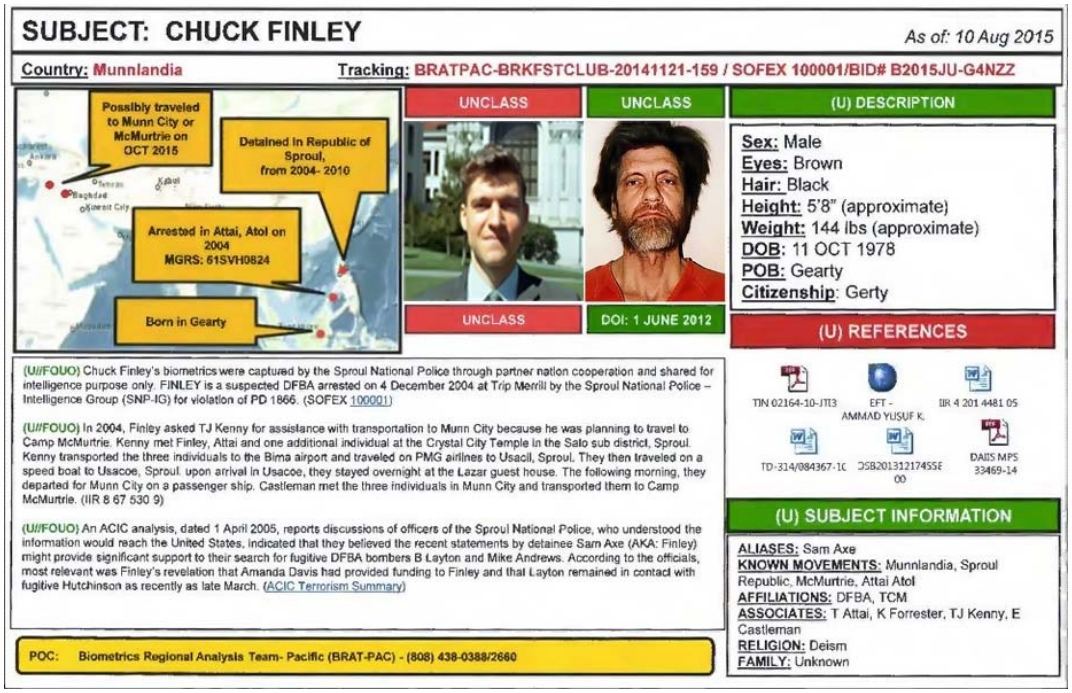

Figure B-1. Sample Pre-Operation Identity Intelligence Tracking Intelligence Package

7. Networks and Identities Assessment

A networks and identities assessment is a written long term intelligence assessment that is typically 3-20 pages in length, and provides in-depth profiles of key persons and networks of interest to the commander. Networks and identities assessments are all-inclusive and describe the character, intentions make-up, capabilities, operational capacity, and reach of operationally relevant networks operating within the commander's operational area.

8. Behavioral Influences Analysis Products

a. **Individual Biography.** A baseline and descriptive analytic product that supports the development of the behavioral influences analysis (BIA) individual behavioral profile and complements the BIA group behavioral profile and organizational behavioral profile. Individual biographies identify the significance of operational-level foreign forces leadership, commanders, and key personnel as well as critical individual roles and responsibilities. IO planners, and US military or diplomatic delegations are the primary audience for this product line.

b. **BIA Individual Behavioral Profile.** An in-depth analysis of a specific operational-level foreign air, space, or missile commander or key unit member focused on assessing command or unit climate and individual decision-making calculi. This product relies heavily on a sophisticated remote profiling methodology and is intended for IO planners.

c. **BIA Group Behavioral Profile.** An in-depth analysis of specific groups within operational foreign air, space, or missile forces focused on assessing group traits, behavioral influences, and potential vulnerabilities within and between groups. Though this product has many applicable audiences, it is written with IO planners in mind.

d. **BIA Organizational Behavioral Profile.** An in-depth analysis of operational-level foreign air, space, or missile units and organizations focused on assessing organizational behavior, and influences on leadership and decision making. This product relies heavily on an organizational psychology-based methodology and is intended for IO planners.

9. Identity Intelligence Support Packet—Pre-Operation

A tailored multi-intelligence technical exploitation product developed to support SOF F3EAD operations and activities. Pre-operation identity intelligence support packet (I2SP) products provide detailed information about threat activity and potential high-threat areas within the OE. These products significantly enhance understanding of where threat actors are operating and the weapons and TTP they may be employing. I2SPs enable improved force protection, targeted operations, enhanced intelligence collection, and coordinated operation planning in a multinational environment. A sample pre-operation I2SP is depicted in Figure B-2.

Sample Pre-Operation Identity Intelligence Support Package

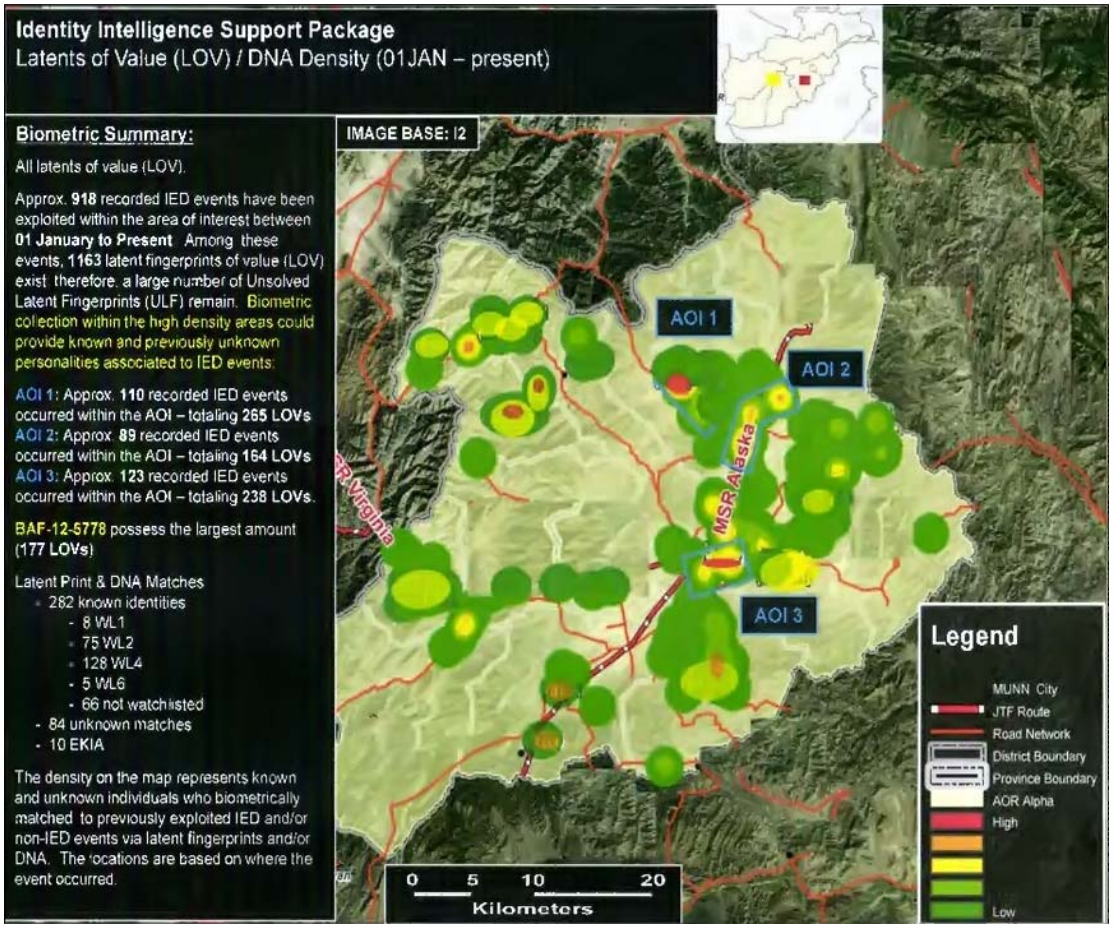

Figure B-2. Sample Pre-Operation Identity Intelligence Support Package

10. Identity Intelligence Support Packet—Post-Operation

A tailored multi-intelligence technical exploitation in support of DOD requirements and F3EAD focusing on I2. Post-operation I2SPs are produced in response to SOF requests for information to support follow-on operational planning. The I2SP provides tailored multi-intelligence technical exploitation in support of SOF F3EAD activities. The I2SP supports location-based analysis, detention operations, and target development. Post-operation I2SP products are typically completed within two weeks of the request, but can be produced more quickly if required. A sample post-operation I2SP is depicted in Figure B-3.

Sample Post-Operation Identity Intelligence Support Package

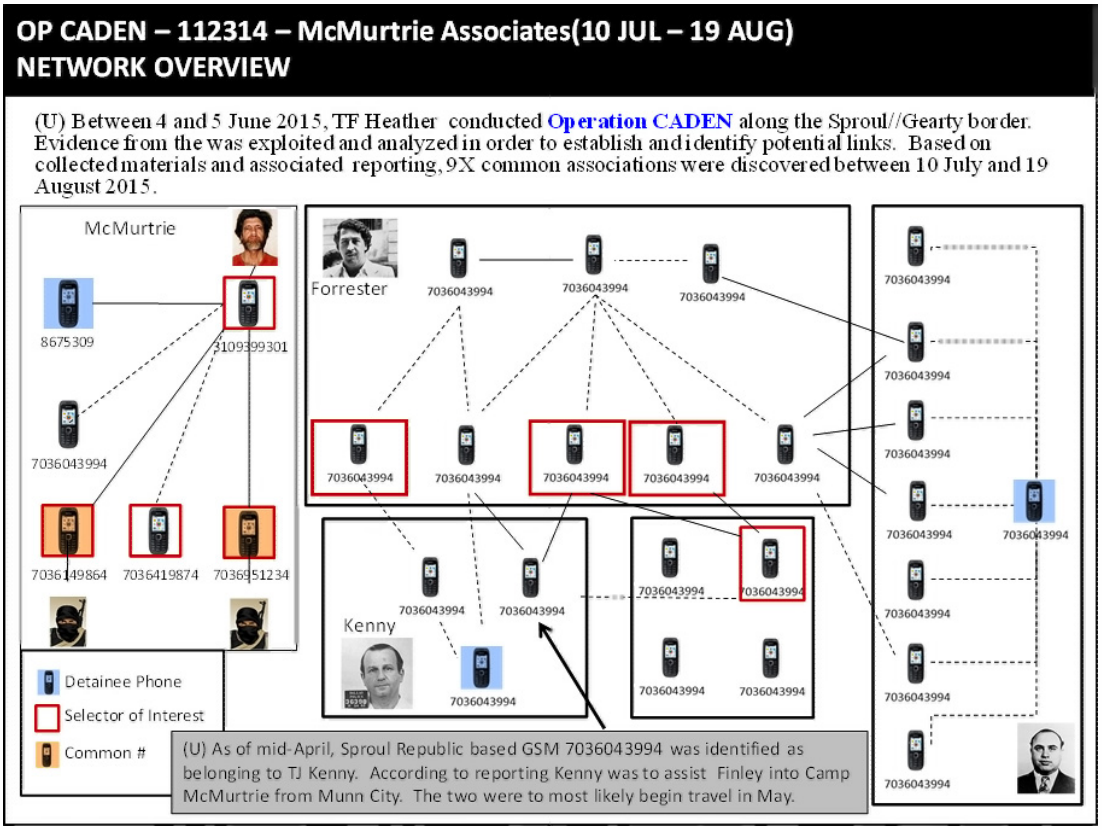

Figure B-3. Sample Post-Operation Identity Intelligence Support Package

11. Person of Interest Packets

Person of interest packets provide analytic support to foreign personnel vetting missions. These packets provide tailored summaries of significant derogatory information on individual persons of interest, combining biometric, cell phone exploitation, and CI screening information in an easily briefed format on foreign nation or HN personnel working with forward deployed military and/or USG personnel. A sample person of interest packet is depicted in Figure B-4.

12. Biometrics Focused Area Studies

A biometrics focused area study is a detailed biometric collections-based geospatial analysis of a specified area of current or future operations. These products enhance operational planning and provide situational awareness of known actors operating in an area. If appropriate, biometric network analysis charts can be included within a focus area study product. See Figure B-5.

Sample Person of Interest Packet

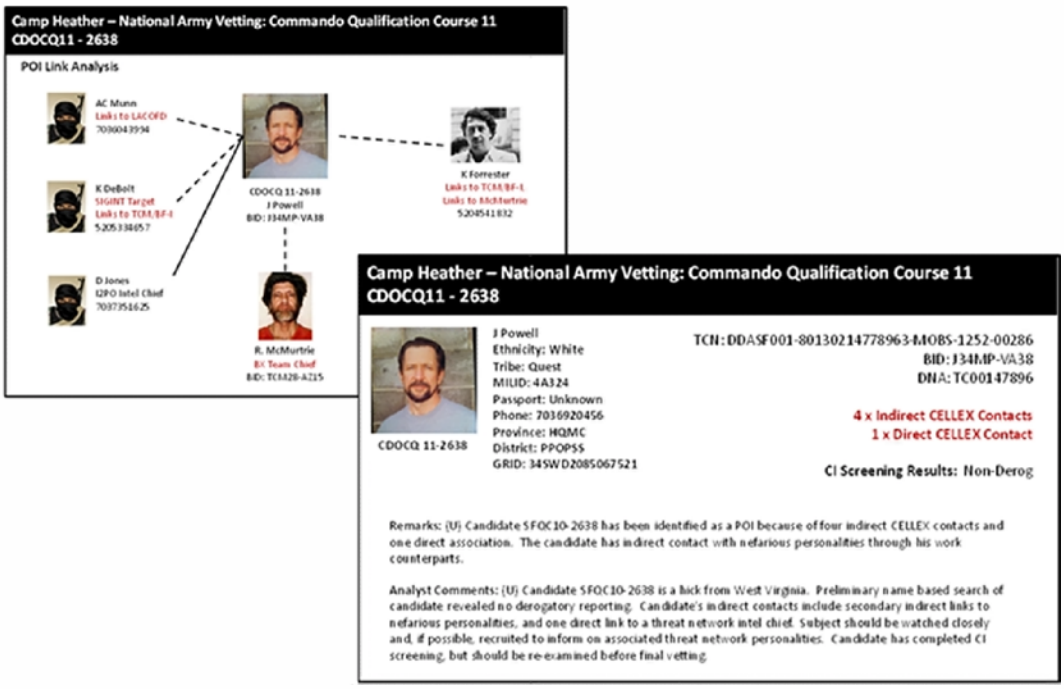

Figure B-4. Sample Person of Interest Packet

13. Identity Intelligence Intelligence Information Reports

I2 intelligence information reports (IIRs) are intelligence reports that provide basic biographical information (including case links) of subjects enrolled by US forces to the IC. I2 IIRs are designed to provide biographic details of subjects biometrically enrolled by military forces in an unclassified product and include a link to the case file or dossier where classified derogatory information on the subject resides.

14. Identity Intelligence Capabilities Assessments

I2 capabilities assessments are written assessments, typically 3-20 pages in length, that address the technical characteristics, capabilities, effectiveness, and vulnerabilities of current, developing, or projected foreign I2 collection, processing, and analytic systems and their related databases.

15. Quiktel

Quicktel is a short assessment that addresses time sensitive emerging, high interest identity, network, and biometric capability topics with limited available collection.

Biometrics Focused Area Studies

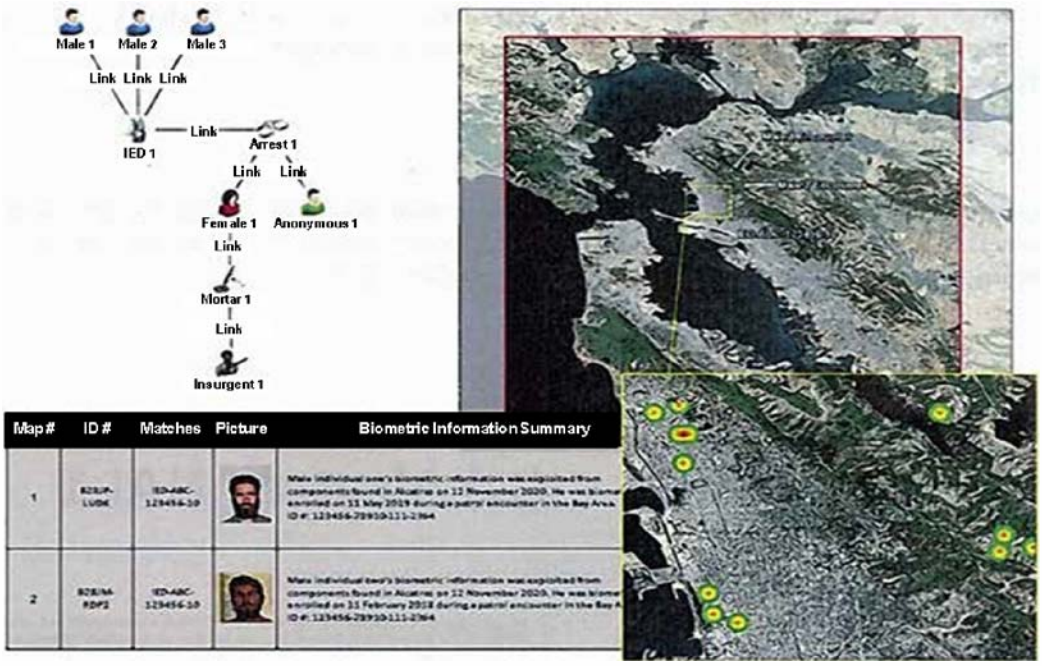

Figure B-5. Biometrics Focused Area Studies

Intentionally Blank

APPENDIX C
ASSESSMENT INDICATORS FOR IDENTITY ACTIVITIES

1. This appendix provides examples of the objectives, effects, and indicators for identity activities. While not all inclusive, it does provide a start point for operation planners. The ultimate use of these measures, as well as additions to, deletions from, and other changes to them is up to the JFC and subordinate commanders.

2. The identity activities assessment indicators listed in the figures follow the guidance provided by JP 5-0, *Joint Planning.* Identity activities feed the operational assessment process and, therefore, must identify the indicators necessary for identity activity planning and execution throughout the range of military operations.

3. Figure C-1 should be considered an umbrella identity activity assessment indicator figure. Additional mission-specific identity activity considerations and indicators are provided in Figures C-2 through C-33.

Example: Objective, Effects, and Indicators for Identity Information and Data (to Include Biometrics, Forensics, and Other Exploitation)

Objective	Effect	Indicator	Data Category	Frequency (example)
Use identity activities to enhance missions throughout the range of military operations.	1. Identity activities are planned for, inserted into operation plans and operation orders, and executed.	1. Ensure bilateral agreements are in place between the US and partners nations (PNs) in order for US forces to collect, store, and share identity (to include biometrics, forensics, and other exploitation) information and data. Include identity activities in theater campaign plans/theater security cooperation planning and that they do not violate any international law or policies (to include the rules of engagement and applicable standard operating procedures in dealing with any local populace).	Qualitative/ Objective	Prior to conducting identity activities within the operational area
		2. Use J-2/G-2 (intelligence planning) and J-3/G-3 (operation planning) to plan for, execute, and assess identity activities (identification and forensic data) that will gather and secure evidence.	Qualitative/ Objective	Planning, execution, and assessment of identity activities as well as collection of forensics and/or other site exploitation activities
		3. Designate indigenous forces, as appropriate, as the lead at every possible opportunity for identity activities.	Qualitative/ Subjective	As appropriate

		4. PN organizations not allowed to assist with gathering of forensic or other exploitation information and/or data, or evidence may be used, upon approval by the PN investigator, to primarily cordon and secure the site.	Qualitative/ Objective	Prior to identity and/or forensic data and/or other site exploitation activities
		5. Identify local leaders and use them to assist in identifying the populace.	Quantitative/ Objective	Once and as required
		6. Create biometric enrollment events for future data mining.	Quantitative/ Objective	Throughout operations
	2. Personnel in the operational area are identified.	1. Ensure unit and/or patrol with handheld collection devices has taken enough extra charged batteries for completion of the mission.	Qualitative/ Subjective	Each collection event
		2. Collect, to standard, identity information (e.g., personal documents, voter registration, driver's licenses, government databases) from individuals, to include detainees, within the operational area.	Quantitative/ Objective	Once
		3. At a minimum, fully biometrically enroll all military age males with full sets of fingerprints, full face photos, iris images, names, and all variants of names.	Quantitative/ Objective	Once
		4. Put identity information for all individuals in a common database.	Quantitative/ Objective	Every encounter
		5. Ensure current watch lists and local alerts are loaded before mission execution.	Qualitative/ Objective	Prior to each mission
		6. Send identity information to the Department of Defense authoritative database for match/no match.	Quantitative/ Objective	Every encounter
		7. Collect, preserve, store, analyze, and share forensic and other exploitation information and data.	Quantitative/ Objective	Each incident
	3. Intelligence functions produce identity intelligence products.	1. All-source intelligence analysts fuse and analyze all identity information from all sources (to include biometrics, personal identity documents, government database, forensics, and other exploitation), Record the following biographic data elements: address, occupation, tribal name, location of enrollment (military grid), to provide identities and trustworthiness attributes for each encountered individual.	Qualitative/ Subjective	Concurrent with all intelligence analysis
		2. Designate biometric named areas of interest through which persons of interest can be tracked.	Quantitative/ Objective	As required during intelligence analysis

		3. Use all sources of identity activities to support Intelligence operations (targeting individuals, cue other intelligence assets, ensure the correct target is engaged).	Qualitative/ Subjective	All opportunities to identify individuals
	4. Personnel are vetted for trustworthiness; to determine whether they are a threat (military, nonmilitary, criminals, terrorists), friendly, or neutral.	1. Compare identity information against the biometrics-enabled watch list for match/no match and actions to take upon a match.	Quantitative/ Objective	Every encounter
		2. Use a badge system to identify local leaders and key personnel.	Quantitative/ Objective	Once and as required

Figure C-1. Example: Objective, Effects, and Indicators for Identity Information and Data (to Include Biometrics, Forensics, and Other Exploitation)

Example: Objective, Effects, and Indicators for Alien Migrant Interdiction Operations				
Objective	Effect	Indicator	Data Category	Frequency (example)
Determine, and vet, identities of interdicted personnel for humanitarian missions and enforcement of US immigration laws at sea.	Assist, as necessary with other government departments or agencies (e.g., Federal Bureau of Investigation, Department of Homeland Security), and local authorities for identification and vetting of migrants as they attempt to enter the US from the sea.	1. Collect identity information and data from all individuals interdicted at sea. See Figure C-1.	See Figure C-1	See Figure C-1

Figure C-2. Example: Objective, Effects, and Indicators for Alien Migrant Interdiction Operations

Example: Objective, Effects, and Indicators for Base Access, Entry Control Points/Ports of Entry/Maritime Interception/Checkpoints				
Objective	Effect	Indicator	Data Category	Frequency (example)
Determine, and vet, identities of all personnel requesting access to bases, facilities, through checkpoints,	1. Authorized personnel are allowed access and exit.	1. Plan and establish checkpoints for identity verification. (yes/no)	Qualitative/ Subjective	As needed
		2. Canalize all traffic to checkpoints. (yes/no)	Qualitative/ Subjective	For all checkpoints
		3. Use "overwatch" to spot individuals trying to avoid checkpoints. (yes/no)	Qualitative/ Subjective	For all checkpoints
		4. Ensure up-to-date biometrics-enabled watch list, for the unit's operational area, is uploaded to the	Qualitative/ Objective	Every day

points of entry, etc.		biometric handheld collection devices for verification.		
		5. Access authority receives personal identity documents from all individuals requesting access.	See Figure C-1	Once, during access authorization
		6. Fully enroll all personnel who will be allowed access to the installation.	Quantitative/ Objective See Figure C-1	Once, during access authorization
		7. Submit all enrollments to the Department of Defense authoritative database to complete the identification process for all locally employed personnel and require a match response.	Quantitative/ Objective See Figure C-1	Once during access authorization
		8. Issue authorized personnel a biometrically enabled access card.	Quantitative/ Objective	Once, upon authorization
	2. Unauthorized personnel are prevented from access or exit.	1. Biometrically screen all personnel entering or leaving the base to verify their identity, even if they possess an access card.	Quantitative/ Objective	Every incidence of entry or exit
		2. Plan for full Electronic Biometric Transmission Specification enrollments of suspect individuals.	Qualitative/ Objective	Every suspect individual attempting entry or exit

Figure C-3. Example: Objective, Effects, and Indicators for Base Access, Entry Control Points/Ports of Entry/Maritime Interception/Checkpoints

Example: Objective, Effects, and Indicators for Census Operations				
Objective	Effect	Indicator	Data Category	Frequency (example)
Understand the identities of the population who live in, work in, or are passing through the operational area.	Provide the identities of the population to determine who normally lives in the operational area, who travels to the operational area for employment, are passing through the operational area, or are other individuals (e.g., threat forces, terrorists and/or criminals) who may be coercing the support of the local populations.	1. Conduct identity activities per Figure C-1.	See Figure C-1	Each census operation
		2. Have staging areas and standard operating procedures for collection operations.	Qualitative/ Subjective	Each census operation
		3. Maintain security at all times and ensure there are personnel search teams at the entry control point for the operation. If necessary, ensure your personnel search teams include females in order to search females.	Qualitative/ Subjective	Each census operation
		4. Listen to and understand residents' problems.	Qualitative/ Subjective	Each census operation
		5. Identify local leaders and use them to assist in the identification of the populace.	Qualitative/ Subjective	Each census operation
		6. Locate and identify every resident. (yes/no)	Qualitative/ Objective	Each census operation
		7. Visit and record every house and business.	Qualitative/ Objective	Each census operation
		8. Collect normal census and identification data from all individuals within the local	Qualitative/ Objective	During each census operation

		operational area. (yes/no)		
		9. Use badges to identify local leaders, and key personnel.	Qualitative/ Objective	Each census operation
		10. Track persons of interest; unusual travel patterns may indicate unusual activities.	Qualitative/ Objective	During intelligence analysis and production of identity intelligence products

Figure C-4. Example: Objective, Effects, and Indicators for Census Operations

Example: Objective, Effects, and Indicators for Civil Affairs				
Objective	Effect	Indicator	Data Category	Frequency (example)
Establish or reestablish the legitimacy of local authorities in activities that build or restore the partner nation's (PN's) capability and capacity. Improve PN capability and capacity to provide public services to its population, thereby enhancing legitimacy of the PN, enhancing force protection, and accomplishing the military objectives.	Accurately identify individuals and families receiving aid (medical care, food, water, material, jobs) through the use of identity activities, controls distribution and helps to eliminate waste and black marketeering, support of stability, counterinsurgency, and other operations dealing with "asymmetric" and "irregular" threats.	1. Conduct identity activities per Figure C-1.	See Figure C-1	Each civil affairs (CA) operation.
		2. Provide joint force protection during identity activities as well as protection of the innocent population within the operational area.	Qualitative/ Subjective	Each CA operation.
		3. Provide identity activities within access control missions (as described in the access control figure above).	Qualitative/ Objective	Each CA operation.

Figure C-5. Example: Objective, Effects, and Indicators for Civil Affairs

Example: Objective, Effects, and Indicators for Countering Weapons of Mass Destruction				
Objective	Effect	Indicator	Data Category	Frequency (example)
Prevent the proliferation of weapons of mass destruction (WMD) by identifying personnel associated with	1. Identify personnel associated with WMD sites.	1. Conduct identity activities per Figure C-1 for all individuals apprehended at WMD sites.	See Figure C-1	During every WMD operation
	2. Identify materials and personnel involved in WMD trafficking.	2. Conduct site exploitation at the site (as described in Figure C-30).	Qualitative/ Objective	During every WMD operation

various storage sites and involved in their trafficking.				

Figure C-6. Example: Objective, Effects, and Indicators for Countering Weapons of Mass Destruction

Example: Objective, Effects, and Indicators for Chemical, Biological, Radiological, and Nuclear Response Operations				
Objective	Effect	Indicator	Data Category	Frequency (example)
To control access to chemical, biological, radiological, and Nuclear (CBRN)-affected areas and to physically control access to residents and authorized personnel only.	Identity activities provide the necessary information for positive control of people to the affected areas.	1. Conduct identity activities per Figure C-1 for all individuals requesting access to CBRN sites.	See Figure C-1	Once for every CBRN incident
		2. Control access to the affected areas with a cordon. Match iris images for all personnel entering and exiting the area against the local database. (yes/no)	Qualitative/ Objective	Every entry/exit
		3. Conduct forensics and site exploitation activities site (as described in Figure C-30).	Qualitative/ Objective	Every CBRN incident

Figure C-7. Example: Objective, Effects, and Indicators for Chemical, Biological, Radiological, and Nuclear Response Operations

Example: Objective, Effects, and Indicators for Cordon Operations				
Objective	Effect	Indicator	Data Category	Frequency (example)
Discover selected personnel or materials.	1. Personnel are discovered and identified.	1. Conduct identity activities per Figure C-1 for all individuals within the cordoned site.	See Figure C-1	Each cordon mission.
		2. Use checkpoints in the cordon to canalize traffic and for collection of identity information via personal identity documents and biometric collection devices.	Qualitative/ Objective	All cordon operations
		3. Plan for positive or negative identification of personnel.	Qualitative/ Objective	All cordon operations
		4. Incorporate identity data into debriefs.	Qualitative/ Subjective	Post-mission cordon operations
		5. Biometrically enroll everyone, to include all wounded in action and killed in action.	Quantitative/ Objective	All cordon operations
	2. Materials are discovered and identified.	Plan for forensic data collection, to include latent fingerprints from materials, document and media exploitation (e.g., exploitation of pocket litter, found documents, found computer and cell phones, sim cards).	Qualitative/ Subjective	All cordon operations

Figure C-8. Example: Objective, Effects, and Indicators for Cordon Operations

Example: Objective, Effects, and Indicators for Counterdrug Operations				
Objective	Effect	Indicator	Data Category	Frequency (example)
Use identity activities to contribute to the dissection of drugs, money, and terrorism.	1. Identify individuals and networks involved in drug activities.	Conduct identity activities per Figure C-1 for all individuals within the cordoned site.	See Figure C-1	During all counterdrug operations
	2. Joint force commanders (JFCs) are able to understand the flow of money, laundering of drug money, etc. supporting drug operations and terrorism	Use identity activities to monitor, detect and interdict drug trafficking throughout the area of operations (especially border and transit zones).	Qualitative/ Subjective	During all counterdrug operations
	3. JFCs engage other countries to cooperate against the counterdrug trafficking and its second- and third-order effects.	Use identity activities to further provide an avenue of engagement for the source countries, providing a context for bilateral cooperation against trafficking and its second- and third-order effects.	Qualitative/ Subjective	During all counterdrug operations
	4. JFCs understand identities of individuals and networks conducting drug activities within banking and information technology (to include social media).	Use identity data from cyberspace sources and all other identity information in order to provide intelligence analysts cumulative data to dissect the links among drugs, money and terrorism, as well as the ancillary cottage industries of false documentation and human trafficking.	Qualitative/ Subjective	During all counterdrug operations

Figure C-9. Example: Objective, Effects, and Indicators for Counterdrug Operations

Example: Objective, Effects, and Indicators for Counter-Improvised Explosive Device Operations				
Objective	Effect	Indicator	Data Category	Frequency (example)
Find and track threat, insurgents, and criminals.	1. Through identity activity support to intelligence analysis, individuals can be tied to various organizations and other human networks.	Conduct identity activities per Figure C-1 to identify individuals and networks involved in the preparation of improvised explosive devices (IEDs).	See Figure C-1	Every opportunity and upon discovery of IED kitchens, discovery of emplaced IEDs, and post-IED detonation
	2. Mobility (route clearing). Route clearing patrols	Conduct identity activities per Figure C-1.	See Figure C-1	Discovery of emplaced IEDs, and post-IED

	identify explosives and other dangers near the route. Forensics is used to examine the device and the area. Identity activities are used to support site exploitation as well as biometric enrollment of nearby onlookers to determine if they are a threat.			detonation

Figure C-10. Example: Objective, Effects, and Indicators for Counter-Improvised Explosive Device Operations

Example: Objective, Effects, and Indicators for Combating Terrorism Operations				
Objective	Effect	Indicator	Data Category	Frequency (example)
Reduce or eliminate terrorism.	Inclusion of identity activities in both antiterrorism and counterterrorism operations.	1. Conduct identity activities per Figure C-1 to identify individuals and networks involved in terrorism.	See Figure C-1	Throughout combating terrorism operations.
		2. Conduct site, and other forensic, exploitation to discover identity information about individuals and networks. See Figure C-1.	Qualitative/ Subjective	All opportunities

Figure C-11. Example: Objective, Effects, and Indicators for Combating Terrorism Operations

Example: Objective, Effects, and Indicators for Counterinsurgency Operations				
Objective	Effect	Indicator	Data Category	Frequency (example)
Reduce or eliminate insurgent activities.	Friendly, neutral, threat, and unknown-affiliated populations are identified.	Conduct identity activities per Figure C-1 to identify individuals and networks involved in insurgencies.	See Figure C-1	All COIN operations

Figure C-12. Example: Objective, Effects, and Indicators for Counterinsurgency Operations

Example: Objective, Effects, and Indicators for Countering Threat Networks				
Objective	Effect	Indicator	Data Category	Frequency (example)
Reduce or eliminate threat networks.	Identify all individuals and associated threat networks impacting the operational environment.	1. Conduct identity activities per Figure C-1 to identify threat individuals and networks.	See Figure C-1	Throughout operations
		2. Conduct site, and other forensic, exploitation to discover identity information about individuals and networks.	See Figure C-1	All opportunities

Figure C-13. Example: Objective, Effects, and Indicators for Countering Threat

Networks

Example: Objective, Effects, and Indicators for Cyberspace Operations				
Objective	Effect	Indicator	Data Category	Frequency (example)
Use identity activities to anticipate, mitigate and deter cyberspace threats.	Identify individuals and threats operating in cyberspace.	1. Conduct identity activities per Figure C-1 to identify individuals and networks identified as threats within cyberspace (to include social media).	See Figure C-1	As available
		2. Use information technology/cyberspace standard operating procedures and tactics, techniques, and procedures to identify virtual personas within cyberspace.	Qualitative/ Subjective	Throughout cyberspace operations
		3. Send cyber-persona information to intelligence for fusion with other identity information and data	Quantitative/ Objective	Throughout cyberspace operations
	Cybersecurity measures are effective.	1. Biometrically enroll all network users.	Quantitative/ Objective	Each user
		2. Ensure all users sign and understand, appropriate information assurance forms.	Quantitative/ Objective	Each user

Figure C-14. Example: Objective, Effects, and Indicators for Cyberspace Operations

Example: Objective, Effects, and Indicators for Defense Operations				
Objective	Effect	Indicator	Data Category	Frequency (example)
Enhance defense objectives with identity activities.	Identity activities determine whether individuals within the operational environment are a threat (e.g., military, nonmilitary, criminal, terrorist, neutral).	Conduct identity activities per Figure C-1 to identify individuals and networks identified as threats.	See Figure C-1	During defense operations

Figure C-15. Example: Objective, Effects, and Indicators for Defense Operations

Example: Objective, Effects, and Indicators for Detainee Operations				
Objective	Effect	Indicator	Data Category	Frequency (example)
Positively manage detainees.	1 Identify detained individuals.	1. Conduct identity activities per Figure C-1 to identify and vet detainees.	See Figure C-1	Throughout detainee operations
		2. Positively identify detainees.	Quantitative/ Objective	Upon detainment
		3. Use biometric enrollments to avoid identification mismatches due to changing and/or multiple versions of names.	Quantitative/ Objective	Upon detainment

	2. Support partner nation law enforcement by indicating linkages between an identified detainee and illicit activities.	1. Confirm whether each detainee is involved in illegal or criminal activities.	Quantitative/ Objective	Upon detainment
		2. Assist host nation prosecution of individuals through identity data matches and linkage to criminal activities.	Quantitative/ Objective	Upon detainment
	3. Manage detainees.	1. Track details of interactions with detainees throughout the detention process to include release (prevent the release of the wrong person).	Quantitative/ Objective	During detainment and prior to release
		2. Prepare for effective tactical questioning and/or interrogation by comparing the detainee's biometric information with the biometrics-enabled watch list and other activities.	Quantitative/ Objective	During detainment

Figure C-16. Example: Objective, Effects, and Indicators for Detainee Operations

Example: Objective, Effects, and Indicators for Counter-Threat Finance Operations				
Objective	Effect	Indicator	Data Category	Frequency (example)
Support partner nation (PN) investigations to identify, prosecute, and counter threat finance operations.	1. Discover identities of those individuals and networks involved in threat finance operations.	1. Conduct identity activities per Figure C-1 to identify and individuals suspected of unlawful threat finance activities.	See Figure C-1	Prior to information and/or data collection
		2. When identifying individuals, also consider virtual personas, and banking institutions databases to include linkage to networks, events, locations, and materials.	Quantitative/ Objective	Throughout operations
	2. Track financial transactions and financial activities.	1. Provide forensic exploitation of digital media; computer hard drives, cell phone histories and subscriber identity module cards (part of the document and media exploitation mission set),	Quantitative/ Objective	Upon discovery of threat finance activities and/or persons/networks
		2. Identify, and plan for, opportunities to interdict funding of illicit activities	Qualitative/ Subjective	In coordination with PNs and discovery of illicit activities
		3. Use forensic techniques to trace financial records and identify financiers	Quantitative/ Objective	In coordination with PNs and discovery of illicit activities

Figure C-17. Example: Objective, Effects, and Indicators for Counter-Threat Finance Operations

Example: Objective, Effects, and Indicators for Foreign Internal Defense Operations				
Objective	Effect	Indicator	Data Category	Frequency (example)
Enhance foreign internal defense (FID) objectives through identity	Identify and vet individuals to support the protection of the	1. Engage with host nation (HN) authorities and provide education on the usefulness of identity capabilities (such as biometrics,	Qualitative/ Subjective	At initiation of FID operations, training, exercises, etc.

activities.	host nation (HN) against subversion, lawlessness, insurgency, terrorism, and other threats to their security.	forensics, and document and media exploitation).		
		2. Ensure bilateral agreements are in place between the US and the HN in order for US forces to collect, store, and share identity (to include biometric and forensic) information and data.	Qualitative/ Objective	Prior to FID operations; if not in place, quickly develop and approve agreements with specifics
		3. Store identity data into a local database.	Quantitative/ Objective	Upon establishment of agreements; prior to initiation of training, exercises, etc.
		4. Verify the identities of individuals receiving US led training (especially through the use of biometrics), and vet, the individual trained against the biometrics-enabled watch list, the Department of Defense authoritative biometrics repository, and/or the local database.	Quantitative/ Objective	Upon establishment of agreements; prior to initiation of training, exercises, etc.

Figure C-18. Example: Objective, Effects, and Indicators for Foreign Internal Defense Operations

Example: Objective, Effects, and Indicators for Human Trafficking				
Objective	Effect	Indicator	Data Category	Frequency (example)
Use identity activities to oppose prostitution, forced labor, and any related activities contributing to the phenomenon of trafficking in persons (TIP).	Reduce the level of human trafficking in commanders' operational areas.	1. Ensure the identification of personnel involved in TIP (victim/suspect).	Quantitative/ Qualitative	Each encounter
		2. Biometrically enroll all TIP violators.	Quantitative	Each encounter
		3. Plan for identity data collection in the operation order/fragmentary orders for any TIP activities.	Qualitative/ Subjective	As available

Figure C-19. Example: Objective, Effects, and Indicators for Human Trafficking

Example: Objective, Effects, and Indicators for Foreign Humanitarian Assistance				
Objective	Effect	Indicator	Data Category	Frequency (example)
Enhance foreign humanitarian assistance (FHA) objectives with identity activities.	1. Joint forces are protected from criminal and possible threat activities.	1. Plan to identify potential persons of interest (Watch listed individuals).	Qualitative/ Subjective	Prior to execution of FHA operations
		2. Detain anyone on the biometrics-enabled watch list (if used) or who has had a latent print recovered from a site of anti-multinational force activities.	Quantitative/ Objective	Every encounter

		3. Plan for full biometrics enrollments and verifications/screenings.	Qualitative/ Objective	Prior to execution of FHA operations
		4. Ensure authorities and agreements are in place with host nations for Department of Defense collection, storage, and sharing of identity information in the partner nations (PNs).	Qualitative/ Objective	Prior to execution of FHA operations
		5. Integrate the identification, verification, and vetting of individuals to better provide joint force protection.	Quantitative/ Objective	Every encounter
		6. Use identity information with regards to base camp organization for access control.	Quantitative/ Objective	Every encounter
	2. Families are reunited due to FHA.	Reunite families after a disaster (using deoxyribonucleic acid).	Quantitative/ Objective	For every separated individual
	3. FHA resources are provided to all persons in need.	1. Biometrically enroll all recipients of FHA to ensure no "double dipping" into FHA resources.	Quantitative/ Objective	Every encounter
		2. Collect identity data from personal identity documents and PN databases (e.g., driver's licensing, voter registration).	Quantitative/ Objective	Every encounter
		3. Provide for more efficient records/organization of individual profiles through the use of identity information	Qualitative/ Subjective	Every encounter
		4. Use identity data for placement and tracking of individuals and resources provided to each individual.	Quantitative/ Objective	Every encounter
		5. Share identity information and data with other agencies and multination partners for the efficient pursuit of the FHA purposes.	Quantitative/ Objective	Every encounter

Figure C-20. Example: Objective, Effects, and Indicators for Foreign Humanitarian Assistance

Example: Objective, Effects, and Indicators for Intelligence				
Objective	Effect	Indicator	Data Category	Frequency (example)
Support identity intelligence products.	Identity activity information and data are integrated throughout all-source intelligence analysis and products.	1. Conduct identity activities to support intelligence analysis per Figure C-1.	See Figure C-1	Throughout military operations
		2. Use all sources of identity activities to support Intelligence operations (targeting individuals, cue other intelligence assets, ensure the correct target is engaged).	Qualitative/ Subjective	All opportunities to identify individuals

Figure C-21. Example: Objective, Effects, and Indicators for Intelligence

Example: Objective, Effects, and Indicators for Logistics				
Objective	Effect	Indicator	Data Category	Frequency (example)
Identity activities enhance logistics support to joint force commanders (JFCs) across the range of military operations.	Identity activities are used to support force freedom of movement, disposition of material, contractor vetting, and tracking of services given to personnel.	1. Conduct identity activities to support logistics per Figure C-1.	See Figure C-1	Throughout JFC operations
		2. Biometrically enroll, and vet, all Department of Defense contractors and locally employed personnel.	Quantitative/ Objective	Each contractor and locally employed personnel
		3. Require biometrics validation to receive payment.	Quantitative	Per standard operating procedures

Figure C-22. Example: Objective, Effects, and Indicators for Logistics

Example: Objective, Effects, and Indicators for Military Police Operations				
Objective	Effect	Indicator	Data Category	Frequency (example)
Use identity activities to enhance military police (MP) operations support to identity intelligence and law enforcement missions as well as possible future prosecutions.	Individuals and/or networks are identified, verified, and vetted to determine whether they are threats of any type.	1. Conduct identity activities to support noncombatant evacuation operations per Figure C-1.	See Figure C-1	During all military operations
		2. Provide MP and exploitation analyses for possible linkage of identified individual and/or network threats to unlawful events, materials, and locations.	Qualitative/Objective Also see Figures C-1 and C-30 (Site Exploitation)	During all military operations

Figure C-23. Example: Objective, Effects, and Indicators for Military Police Operations

Example: Objective, Effects, and Indicators for Noncombatant Evacuation Operations				
Objective	Effect	Indicator	Data Category	Frequency (example)
Enhance noncombatant evacuation operations (NEOs).	Use identity activities to identify those eligible for NEO.	Conduct identity activities to support NEOs per Figure C-1.	See Figure C-1	Each encounter

Figure C-24. Example: Objective, Effects, and Indicators for Noncombatant Evacuation Operations

Example: Objective, Effects, and Indicators for Offense Operations				
Objective	Effect	Indicator	Data Category	Frequency (example)
Enhance offense operations objectives with identity activities.	Identity activities determine whether individuals within the operational	1. Conduct identity activities per Figure C-1.	See Figure C-1	Throughout offense operations as appropriate.
		2. Ensure detainees within the	See Figure	Throughout

	environment are a threat (military, non-military, criminal, terrorist, neutral).	area of responsibility and/or suspect individuals are identified and vetted for trustworthiness.	C-1	offense operations as appropriate

Figure C-25. Example: Objective, Effects, and Indicators for Offense Operations

Example: Objective, Effects, and Indicators for Peace Operations				
Objective	Effect	Indicator	Data Category	Frequency (example)
Enhance peace operations objectives with identity activities.	Identities of individuals and/or networks are verified and vetted for trustworthiness.	1. Conduct identity activities, per Figure C-1, for partner nation (PN) individuals, networks, local police, military, and security forces, as well as those to receive training.	See Figure C-1	Throughout peace operations as appropriate
		2. Use identity activities as a means to work more closely with PN forces and organizations managing food, water, medical care, funds, contractor, etc.	Qualitative/ Subjective	As mission allows
		3. Inform commanders about the true background of some of PN personnel, potential hires, civilian population (e.g., medical).	Qualitative/ Subjective	Each applicant

Figure C-26. Example: Objective, Effects, and Indicators for Peace Operations

Example Objective, Effects, and Indicators for Personnel Recovery				
Objective	Effect	Indicator	Data Category	Frequency (example)
Use identity activities to enhance personnel recovery operations.	Identify recovered persons (alive, deceased, or unconscious).	1. Conduct identity activities, per Figure C-1, for recovered individuals (alive, deceased, or unconscious).	See Figure C-1	Throughout operations
		2. Positively identify a person that is alive, deceased (regardless of the integrity of the body), or if the individual is unconscious.	Quantitative/ Objective	Each encounter

Figure C-27. Example Objective, Effects, and Indicators for Personnel Recovery

Example Objective, Effects, and Indicators for Personnel Screening and Vetting				
Objective	Effect	Indicator	Data Category	Frequency (example)
Enhance force protection and local security.	Identify, verify identities, and vet personnel (threat, friendly, or neutral) to determine allegiance, background or suitability for credentialing, decide access to a protected area (e.g., base, town, or	Conduct identity activities, per Figure C-1, for personnel.	See Figure C-1	Throughout operations

	to possibly segregate populations to enhance security.			

Figure C-28. Example Objective, Effects, and Indicators for Personnel Screening and Vetting

Example Objective, Effects, and Indicators for Populace and Resources Control Measures				
Objective	Effect	Indicator	Data Category	Frequency (example)
Enhance the management of local populations during operations throughout the range of military operations.	Identity, verify, and vet the identities of the population in order to deny freedom of movement and provide resources to designated population.	1. Conduct identity activities, per Figure C-1, for personnel.	See Figure C-1	Throughout operations
		2. Plan, and establish, checkpoints for identity verification.	Quantitative/ Objective	Throughout operations

Figure C-29. Example Objective, Effects, and Indicators for Populace and Resources Control Measures

Example Objective, Effects, and Indicators for Site Exploitation				
Objective	Effect	Indicator	Data Category	Frequency (example)
Use identity activities to enhance sire exploitation (SE) for identity intelligence and law enforcement missions as well as possible future prosecutions.	Properly record and preserve the evidence.	1. Conduct identity activities per Figure C-1.	See Figure C-1	See Figure C-1
		2. Collect and preserve latent fingerprints. (yes/no)	Qualitative/ Objective	Each occurrence
		3. Compare latent fingerprints against authoritative repositories and the biometrics-enabled watch list. (yes/no)	Qualitative/ Objective	Each occurrence
		4. Add identity information from this specific SE to dossiers on involved individuals. (yes/no)	Qualitative/ Objective	Each occurrence
		5. Security teams ask individuals at the SE site to show their identification documents as well as enrolled/matched with biometric devices.	Qualitative/ Objective	Each occurrence
		6. Tag, record, package, and transport useful artifacts, electronic data/media, fibers, and other documents to the nearest forensic laboratory. (yes/no)	Qualitative/ Objective	Each occurrence
		7. Follow strict chain-of-custody policies for all artifacts and documents. (yes/no)	Qualitative/ Objective	Each occurrence
		8. Retain and exploit all useful artifacts and documents for intelligence value and/or prosecution efforts. (yes/no)	Qualitative/ Objective	Each occurrence

Figure C-30. Example Objective, Effects, and Indicators for Site Exploitation

Example Objective, Effects, and Indicators for Stability Operations				
Objective	Effect	Indicator	Data Category	Frequency (example)
Enhance stabilization, security, transition and reconstruction operations.	Identify, verify, and vet individual identities in order to evaluate trustworthiness and identify threats (criminals, terrorists, insurgents), friendly, and neutral entities and/or networks within the population.	1. Conduct identity activities per Figure C-1.	See Figure C-1	See Figure C-1
		2. Use identity activities as a means to work more closely with host nation forces (e.g., elections, food, water, medical care, funds, contractor employment, and distribute resources).	Quantitative/ Subjective	As mission allows
		3. Inform commanders about the true background of some of their personnel, potential hires, civilian population (e.g., medical).	Qualitative/Subjective	Each applicant

Figure C-31. Example Objective, Effects, and Indicators for Stability Operations

Example Objective, Effects, and Indicators for Support to Targeting				
Objective	Effect	Indicator	Data Category	Frequency (example)
Enhance targeting.	1. Identity activities determine high-value individuals that may be nominated for targeting.	1. Conduct identity activities per Figure C-1	See Figure C-1	See Figure C-1
		2. After consideration of all operational factors, and staff input, joint force commanders identify potential high-value individuals for targeting (lethal and/or non-lethal effects).	Qualitative/Subjective	All operations throughout the range of military operations
	2. During or post-targeting mission, identity activities are used in the verification of the identity of each targeted individual.	3. Use biometrics to verify target(s).	Quantitative/ Objective	As occurs

Figure C-32. Example Objective, Effects, and Indicators for Support to Targeting

APPENDIX D
IDENTITY ATTRIBUTES AND SUB-ELEMENTS

1. Biographical

a. **Personal Name**

(1) A given name (also known as a personal name, first name, forename, or Christian name) is a part of a person's full nomenclature. It identifies a specific person, and differentiates that person from other members of a group, such as a family or clan, with whom that person shares a common surname.

(a) Mononyms. In some societies, it is common for individuals to be given only one name. Across the world certain, individuals, such as royalty or prominent artists, entertainers, writers, and musicians assume the use of only one name.

(b) Polynym. Connotes an individual who has multiple names.

(2) A surname is a name added to a given name. In many cases, a surname is often referred as a family name.

(a) In some cultures, individuals do not have surnames.

(b) In the many western societies, "surname" is often synonymous with "last name," since it is usually placed at the end of a person's given name. However, in many Asian societies the surname precedes the given name.

(c) Individuals may also possess two distinct surnames, which is common in Spanish speaking countries where the first surname is the father's family name and the second surname is the mother's family name. The order can be a choice in some cultures. Individuals may also drop either one of the surnames.

(d) Surnames can be compound surnames which feature two or more words with or without hyphen(s).

(e) In some cultures the surname can be gender specific and contain a feminine suffix used by the wife and unwed daughters and a masculine suffix used by the husband/father and sons.

(f) Upon marriage in many cultures, women may assume their husband's surname, but do not always do so.

(3) Patronymics or matronymics are used to convey lineage, as a component of an individual's name. These naming conventions consist of the name of an ancestor (e.g., father, mother, grandfather, grandmother) with the addition of a prefix or suffix. Arabic naming conventions follows that the individual will have a given name, followed by father's given name, for example then the grandfather's given name.

(a) An individual may be assigned patrilineal and matrilineal names to denote family history.

(b) Many Arabic, Turkish, Persian, Urdu and some Southern Asian societies names may contain one or more "nisba," which is an adjective denoting the person's place of origin, tribal affiliation, or ancestry.

(c) An individual's name may change to either mask or promote their ethnicity or mark a religious transition.

(4) Pseudonyms (a name that a person assumes for a particular purpose).

(a) Nicknames (i.e., name given to them by friends or family).

(b) Alias or false name, used to hide their identity.

(c) Cultural or organizational given names.

(d) Nom de guerre (i.e., name one assumes to fight, sometimes reflecting the person's place of origin, and also used for security reasons to protect family or to break from their past).

(e) Screen names, pen name, or stage name (i.e., names used to mask an individual's private life, gender, or ethnic origins; names assigned by guild or sponsor; or names used to prevent confusion or when the true name is considered unsuitable).

(f) Cyberspace names (e.g., gamer identifications, code names, hacker handles, user name, login name, avatar, cyber-persona, or superhero identities).

b. **Identity Documents.** Any document which may be used to verify aspects of a person's identity, which may include the owner's full name, a portrait photo, age, date of birth, address, an identification number, profession, religion, ethnic or racial classification, restrictions, and citizen status. Much of this personal information is stored on centralized governmental databases. Many countries are leveraging biometrics and smart card technologies into these documents for greater security against fraudulent use and multiuse conveniences.

(1) **National Identification Card.** Approximately a hundred countries have identity cards. Many of these countries are employing or will soon be using smart card technologies in these cards. A national smart identification card would incorporate an embedded digital chip which can contain certain biometric data and enhance its security. With smart cards, many countries have expanded the role of these cards beyond identification, to also being a credit card, debit card, voter card, and driver's license. A national identity card is used by governments as a means of tracking their citizens, permanent residents, and temporary residents for the purposes of work, taxation, government benefits, health care, and other related functions. Several countries also use the national identity card to impose certain control measures such as its possession being a requirement to

purchase gasoline, open or close bank accounts, and obtain a mobile phone subscriber identity module card.

(2) A passport is a travel document that certifies the identity and nationality of its holder for the purpose of international travel.

(3) A driver's license or driving license is an official document that entitles a person to operate a prescribed motor vehicle. Those countries that lack national identification cards tend to use the driver's license as a standard form of identification. Whereas those countries with national identification cards typically do not accept driver's license as a valid form of identification.

(4) Other forms of identification may include employee identification cards, academic identification cards, access badges, voter registration cards, birth certificates, library cards, vehicle registrations, ration books, church/baptismal records, and utility records.

(5) An internment serial number is a unique identification number assigned to each EPW, retained personnel, and civilian internee taken into the custody of the Armed Forces of the United States.

c. **Addresses**

(1) A residential mailing address is a collection of information, presented in a mostly fixed format, used for describing the location of a building, apartment, or other structure or a plot of land, generally using political boundaries and street names as references, along with other identifiers such as house or apartment numbers.

(2) An individual may have one or more current residences as well as former residences. A residence may house an individual, a family, or several families. A mailing address can be a post office box.

(3) With close to a billion people currently residing in slum settlements across both developed and developing countries, the complexities of dense urban terrain pose a significant challenge to acquiring proper addresses. Often located on the most undesirable land, such as poor agricultural areas, flood zones, and near city dumps, the slum areas, shanty towns, and squatter areas often occupy both the intercity and the periphery of urban areas. These areas typically lack proper road infrastructure, public services, and housing. Tents and shacks are often quickly installed without legal property rights or adherence to proper building codes resulting in homes that are not registered or recognized by local or state governments.

(4) Other challenges come from over 100 million persons worldwide that are homeless. Homeless persons are those individuals living on the streets without a shelter that would fall within the scope of living quarters and those with no place of usual residence, who move frequently between various types of accommodations (including dwellings, shelters and institutions for the homeless or other living quarters).

(5) The joint force responding to natural disasters typically, will find individuals with former residence(s) that may have been destroyed. Aside from those affected by natural disasters; others may be economic, political, and social refugees, and/or displaced persons whose former residence(s) may have been destroyed or abandoned.

d. **Telephone Numbers.** Telephone numbers could be associated with individuals from a number of sources, home of residence, work, cell phone, etc.

e. **Employment.** May include names of current and past employers, the type of work performed (with econometric or government codes if known), and identifying and locational data such as previous employment, current employment, self-employed, multiple employers, and/or contractual employers.

f. **Educational.** Education background for an individual can be from numerous sources such as recently attended institutions; courses of study; degrees granted; dates of attendance and graduation; professional and vocational certifications.

g. **Military Service.** The specifics of service, such as branch, dates of services, discharge, current status, training, operational experience, etc.

h. **Family.** Covers an individual's relatives, including spouse(s), children, stepchildren, adoptees, parents, step-parents, grandparents, siblings, half-siblings, and step-siblings (and in the latter two instances, the marital basis of the relationships), uncles, aunts, and cousins as well as relatives by marriage (i.e., in-laws). This category accommodates pre-existing familial relationships, an important factor in many cultures.

i. **Cohabitants.** Any other person who lives with an individual and who is not a relative or whose familial relationship status is unknown. This may include boarders, guests, servants, employees (domestic or otherwise), etc.

j. **Acquired Traits.** Characteristics that an individual may have that reflect their education, the skills they have acquired, or their particular interests. This also may include known tastes, the use of specific terms or vocabulary, professional/vocational traits; educational background; demonstrated abilities; attested phobias; attested tastes; and/or recreational preferences or avocations.

k. **Social Affiliation.** A social affiliation can be as the individual self-identifies or as the individual is identified by others: for example, association with religion; race/ethnicity; tribe/other ethnic division; and/or language/dialects.

2. Biological

Biological attributes contain the observable and measurable physical characteristics of an individual.

a. **Physiological Characteristics.** Intrinsic characteristics related to the appearance or shape of the body. Some examples include:

(1) **Iris.** The iris is a flat, colored, ring-shaped membrane behind the cornea of the eye, with an adjustable circular opening (pupil) in the center. An observable physical characteristic is eye color. Iris recognition is an automated biometric method that uses a mathematical pattern-recognition technique to analyze the random pattern of the iris to base identity.

(2) **Face.** The front part of a person's head from the forehead to the chin. The human mind has extraordinary capacity to recognize faces through observation. Facial recognition is an automated biometric application that identifies or verifies a person's identity from a digital source using sophisticated mathematical representation and matching process.

(3) **Finger.** Each of the four slender jointed parts attached to either hand (or five if the thumb is included). Fingers do not typically have observable characteristics. Forensically and biometrically, fingerprints are the impressions left by the friction ridges of the human finger. Fingerprint recognition can be an automated biometric application based on a digital template or forensically relying upon a comparison match by a latent print examiner. This information combines ridge flow, ridge characteristics, and ridge structure of the raised portion of the epidermis.

(4) **Palm Print.** Palm identification, just like fingerprint identification, is based on the aggregate of information presented in a friction ridge impression.

(5) **DNA.** DNA is present in nearly every cell of the human body, and it is unintentionally left behind on anything that has come in contact with the person. The benefit of using DNA as a biometric identifier is the level of accuracy offered: with the exception of identical twins, the chance of two individuals sharing the same DNA profile is less than one in a 100 billion. Because of this accuracy, and recent innovations in processing, DNA profiling has become the mainstay of forensics.

(6) **Voice.** The sound produced in a person's larynx and uttered through the mouth, as speech or song. Humans have an innate skill to recognize a speaker's voice under certain conditions. Often humans apply "multiple sensory modality" by employing both voice recognition and facial recognition seamlessly. Speaker or voice recognition is a biometric modality that uses an individual's voice for recognition purposes. The voice recognition process relies on features influenced by both the physical structure of an individual's vocal tract and the individual's behavioral characteristics.

(7) **Dental.** Forensically, dental records are used to aid the identification of victims of criminal acts, mass fatalities, or missing persons. Teeth have the ability to survive decomposition and withstand extreme climate conditions, making dental examination a very dependable and reliable method for identification. Teeth can also provide information as to the age of the person.

(8) Other common observable physical characteristics:

(a) Gender.

(b) Age (estimated or actual).

(c) Height (estimated or actual; characteristics: short, tall, average, petite).

(d) Weight (estimated or actual).

(e) Facial hair (e.g., no facial hair, beard, mustache, sideburns, goatee).

(f) Race.

(g) Skin tone/complexion (characteristics: dark, light, fair, olive, pale, tan, freckles, spots).

(h) Hair color (i.e., blond, red, black, brown, grey, white) and length (e.g., long, short, receding, bald) and style (e.g., curly, straight, frizzy).

(i) Eye color.

(j) Build (e.g., slim, stocky, thin, fat).

b. **Identifying Marks.** Law enforcement has used identifying scars, marks, and tattoos to identify and verify identities of subjects for over a hundred years. This type of matching process is subjective and very time-consuming. Sources for electronic capture include digital still and video cameras. Scanners are used to digitize sketches, photographs and pictures. Information technologies have enabled machine-readable media to improve the search and matching. Collection and storage of this data requires the entry of mandatory standardized and optional items.

(1) Body modification is the deliberate altering of the human body or physical appearance. The reasons vary according to culture to achieve aesthetics, sexual enhancement, signify a rite of passage, exhibit a religious belief, to display group membership or affiliation, to create art, self-expression, or for the shock value. Body modification involves ear piercing, body piercing, neck ring, tattooing, surface piercing, micro-dermal implants, and transdermal implants.

(a) Ritual scarification involves the scratching, etching, burning, branding, or superficially cutting of designs, pictures, or words into the skin as a permanent body modification.

(b) Tattoos.

(c) Piercings are a form of body modification in which some part of the body is cut or punctured to allow jewelry to be worn. Lip stretching to adorn plates or plugs is also included as piercing.

(2) Deformities and or medical conditions (e.g., blindness, cataract, cleft lip, crippled hand, missing limb or appendage, tuberculosis, leprosy, emphysema, drug use).

(3) Birth marks, skin discolorations, and blemishes (e.g., moles, birth marks, skin discolorations, extra finger/toe, freckles).

(4) Insertions (e.g., gold/silver tooth, orthopedic screw or pin, hair implants, vascular prosthesis).

(5) Medical devices (e.g., artificial prosthetic device, dentures, hearing aid, glasses, cane/walker).

3. Behavioral

a. Behavior refers to the array of every physical action and observable emotion associated with individuals. Behavioral attributes is a range of actions and mannerisms made by an individual in conjunction with themselves or their environment. It reflects an individual's internal or external, conscious or subconscious, overt or covert and voluntary or involuntary responses. Some behavior changes with age, while some specific traits such as personality and temperament may be consistent.

b. Some behavioral characteristics may be obtained from establishing certain patterns from an individual's financial, legal, personal and/or social transactions. These behavioral attributes are more problematic to track and make sense of because humans regularly change their behavior, sometimes radically, when they experience a particular life event. These changes can be as dramatic as quiet Chinese parents who become impassioned protesting radicals when their child is killed in a building collapse during an earthquake, to more typical behavioral shifts that occur after a birth, marriage, or divorce.

c. Predictive behavioral modeling is used to determine the future behavior based on past behavior. On the individual level, this is the analysis of behavior attributes that identify recurring patterns of behavior. Recurring patterns of behavior includes distinctive patterns such as certain repetitive money transactions, social interactions, or even a daily ritual of taking an evening stroll through the park. This type of analysis establishes a pattern of life.

d. On a social behavioral level, this analysis provides certain common human behavioral characteristics. It has been used to detect potentially deceptive behavior such as a polygraph test. Ongoing efforts in behavioral analytics will provide advance warning indicators of potential insider threats, suicide bomber, a saboteur, or spy to alert security forces or cue intelligence sensors.

(1) **Social and Cultural Traits.** Group level traits possess noticeable complex group-level organization and established or emergent norms. Individuals have specialized roles and functions and have established relationships make the group greater than the total sum of individuals within the group. In large groups, individuals may assume unique or blended linguistic distinctions, gender roles, or ritual signs such as tattoos scarification, jewelry, or clothing.

(2) **Human Behavioral Trait.** Describes the particular way in which a person moves, such as their gait, their micro-gestures, their typing rhythm, etc. (speech rhythm; handwriting; type/keyboard pattern; posture/bearing; gait/limp; gestures).

(3) **Financial Transactions.** Any personal transaction information that touches on money, currency, accounts, and wealth.

(4) **Social Transactions**

(a) The term associates refers to patterns of interaction between one individual and other individuals and of one person to groups of people. These patterns may be observed in: E-mails; correspondence; mobile phone call histories; professional networking sites; dating sites; social networking sites; address books; and/or residents in a non-gaming virtual world.

(b) Cyberspace behavior establishes patterns in frequently visited sites, for example extremist websites, online purchasing, online gaming, etc.

(5) Commercial transactions relates to observable patterns in the conduct of commerce and communications.

(6) Media consumption or production relates to patterns in purchasing or creating print and audio/visual channels, as well as online/Internet media content types.

(7) Travel and movement (business, vacation, frequent destinations, tolls, fares passes, work locations).

(8) Telecom records: calling cards; instant messaging service; connectivity; call history; cell phone; landline phone; photos/videos uploaded; geotagging (e.g., geo-browsing, geo-tagged photo, text messages, etc).

4. Reputational

Reputation attributes involve how the individual is objectively or subjectively judged by others. The reputational identity is obtained by interviewing or questioning neighbors, colleagues, leaders, and others with personal knowledge of an individual. Reputation is also collected from individuals with little or no personal knowledge of the individual, but have witnessed or observed what is believed to be the individual conducting certain activity, being at a specific location, or associating with a certain group.

a. **Public records** information connected with the processes of the law and government.

(1) **Judicial.** Addresses outstanding arrest warrants, criminal record, criminal investigations, law enforcement patrol logs, and civil actions, if any.

(2) **Public documents** could include marriage/divorce documents; vehicle registration/tag; employment/business permits; land deeds; construction permits; weapon registration/permits; property tax records, etc.

b. **Financial (historical).** Includes any third-party judgment of historical personal transaction information that touches on money, currency, accounts, and wealth (e.g., credit reports).

c. **Community.** Includes local positions of authority, professional titles, socio-economic status, and/or the knowledge or feelings of neighbors and co-workers.

d. **Social Affiliations.** Descriptive facts that may be attributed to an individual, such as an association or relationship with a religion (with specifics), a tribe or other ethnic division, or other group. It also may include professional and recreational memberships and associations.

e. **Medical and Health**

(1) Health care provider.

(2) Alcohol/drug dependency/rehabilitation.

f. **Electronic Devices**

(1) Application profiles.

(2) Laptop profile.

(3) Personal computer profile.

g. **Military and Security Forces**

(1) Military patrol spot reports (e.g., patrol observations and encounters).

(2) Third-party sworn statements (e.g., interviews and questioning).

(3) IIRs (e.g., interviews and interrogations).

Intentionally Blank

APPENDIX E
REFERENCES

The development of *Joint Doctrine Note X-XX* is based upon the following references:

1. General

a. Title 5, USC.

b. Title 10, USC.

c. Title 50, USC.

2. Strategic Guidance and Policy

a. The National Security Strategy of the United States of America.

b. National Defense Strategy of the United States of America.

c. National Intelligence Strategy of the United States of America.

d. National Military Strategy.

e. National Strategy for Counterterrorism.

f. National Strategy to Combat Transnational Organized Crime.

g. National Strategy for Homeland Security.

h. HSPD-6, *Integration and Use of Screening Information to Protect Against Terrorism.*

i. HSPD-10, *Biodefense for the 21st Century.*

j. HSPD-11, *Comprehensive Terrorist-Related Screening Procedures.*

k. NSPD-59/HSPD-24, *Biometrics for Identification and Screening to Enhance National Security.*

l. PPD 18, *Maritime Security Policy.*

m. PPD 23, *Security Sector Assistance.*

n. EO 12333, *United States Intelligence Activities.*

o. ICD 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community.*

p. ICD 302, *Document and Media Exploitation (DOMEX).*

q. National Disclosure Policy.

r. Department of Defense, Sustaining US Global Leadership: Priorities for 21st Century Defense, January 2012.

3. Department of Defense Publications

a. DODD 3000.07, *Irregular Warfare (IW).*

b. DODD 3300.03, *DOD Document and Media Exploitation (DOMEX).*

c. DODD 5200.27, *Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense.*

d. DODD 5205.14, *DOD Counter Threat Finance Policy.*

e. DODD 5205.15E, *DOD Forensic Enterprise (DFE).*

f. DODD 5240.01, *DOD Intelligence Activities.*

g. DODD 8521.01E, *Department of Defense Biometrics.*

h. DODI 3000.05, *Stability Operations.*

i. DODI O-3300.04, *Defense Biometric Enabled Intelligence (BEI) and Forensic Enabled Intelligence (FEI).*

j. DODM 5200.1, *DOD Information Security Program, Volumes 1-4.*

k. DOD 5400.11-R, *Department of Defense Privacy Program.*

4. Chairman of the Joint Chiefs of Staff Publications

a. JP 1, *Doctrine for the Armed Forces of the United States.*

b. JP 2-0, *Joint Intelligence.*

c. JP 2-01, *Joint and National Intelligence Support to Military Operations.*

d. JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment.*

e. JP 3-0, *Joint Operations.*

f. JP 3-05, *Special Operations.*

g. JP 3-05.1, *Unconventional Warfare.*

h. JP 3-06, *Joint Urban Operations.*

i. JP 3-07, *Stability Operations.*

j. JP 3-07.2, *Antiterrorism.*

k. JP 3-07.3, *Peace Operations.*

l. JP 3-07.4, *Counterdrug Operations.*

m. JP 3-08, *Interorganizational Coordination During Joint Operations.*

n. JP 3-10, *Joint Security Operations in Theater*.

o. JP 3-12, *Cyberspace Operations.*

p. JP 3-15.1, *Counter-Improvised Explosive Device Operations.*

q. JP 3-16, *Multinational Operations.*

r. JP 3-20, *Security Cooperation.*

s. JP 3-22, *Foreign Internal Defense.*

t. JP 3-24, *Counterinsurgency.*

u. JP 3-25, *Countering Threat Networks.*

v. JP 3-26, *Counterterrorism.*

w. JP 3-29, *Foreign Humanitarian Assistance.*

x. JP 3-40, *Countering Weapons of Mass Destruction.*

y. JP 3-50, *Personnel Recovery.*

z. JP 3-57, *Civil-Military Operations.*

aa. JP 3-63, *Detainee Operations.*

bb. JP 3-68, *Noncombatant Evacuation Operations.*

cc. JP 5-0, *Joint Planning.*

dd. Joint Doctrine Note 1-13, *Security Force Assistance.*

ee. Joint Doctrine Note 1-15, *Operation Assessment.*

5. Service Publications

a. Army Doctrine Publication 2-0, *Intelligence*.

b. Army Doctrine Publication 3-0, *Unified Land Operations.*

c. Army Doctrine Publication 3-07, *Stability.*

d. Army Doctrine Publication 3-37, *Protection*.

e. Army Techniques Publication (ATP) 2-19.4, *BCT Intelligence Techniques.*

f. ATP 2-22.82, *Biometrics Enabled Intelligence (BEI).*

g. ATP 3-90.15, *Site Exploitation.*

h. Field Manual (FM) 2-0, *Intelligence.*

i. FM 3-24/Marine Corps Warfighting Publication 3-33.5, *Insurgencies, and Countering Insurgencies.*

j. FM 3-55, *Information Collection.*

k. Marine Corps Doctrinal Publication (MCDP) 1-0, *Marine Corps Operations.*

l. MCDP 5, *Planning.*

m. MCIP 3-17.02, *MAGTF CIED Operations.*

n. Marine Corps Order 5530.17, *Marine Corps Identity Operations (IdOps).*

o. NTTP 3-07.11M/CGTTP 3-93.3/MCIP 3-33.04, *Visit, Board, Search, and Seizure Operations.*

p. USSOCOM Publication 1, *Doctrine for Special Operations.*

q. USSOCOM Directive 525-16 (S/NF), *Preparation of the Environment.*

r. USSOCOM Directive 525-40, *Identity Intelligence Operations.*

s. USSOCOM Directive 525-89 (S/NF), *Unconventional Warfare*.

t. Defense Intelligence Agency and Joint IED Defeat Organization Handbook, *Weapons Technical Intelligence Handbook*, 2014.

6. Allied Publications

a. Allied Joint Publication 2.5, *Captured Persons, Materiel and Documents.*

b. Allied Joint Publication 3.15, *Allied Joint Doctrine for Countering-Improvised Explosive Devices.*

c. Allied Intelligence Publication 15, *Countering Threat Anonymity: Biometrics in support of Operations & Intelligence.*

d. NATO Standardization Agreement 4715, *NATO Biometrics Data, Interchange, Watchlisting and Reporting.*

7. Other Publications

a. Arreguin-Toft, Ivan. "How the Weak Win Wars: A Theory of Asymmetric Conflict," *International Security* (Summer 2001), Vol. 26, No. 1, pp. 93-128.

b. Hammes, Thomas X. "Countering Evolved Insurgent Networks," *Military Review* (July-August 2006), pp. 20-21.

c. Barak, Oren. "Dilemmas of Security in Iraq," *Security Dialogue,* Vol. 38, No. 4, December 2007.

d. Hoffman, Frank G. *Conflict in the 21st Century: The Rise of Hybrid Wars.* Arlington: Potomac Institute for Policy Studies, 2007.

e. Flynn, Michael T., and Charles A. Flynn. "Integrating Intelligence and Information," *Military Review* (January-February 2012).

f. Flynn, MG Michael, M. Pottinger, and P. Batchelor. *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan.* Center for New American Security (January 2010).

g. McFate, Montgomery, and Steve Fondacaro. "Reflections on the Human Terrain System During the First Four Years," *PRISM Journal,* Vol. 2, No. 4 (September 2011).

h. Olson, Wm. J. "War Without a Center of Gravity: Reflections on Terrorism and Post-Modern War," *Small Wars and Insurgencies,* Vol. 18, No. 4 (December 2007).

i. *US Military Response to the 2010 Haiti Earthquake.* RAND Arroyo Center, 2013.

j. Networks and Netwars The Future of Terror[ism], Crime, and Militancy, Edited by John Arquilla, David Ronfeldt.

k. Alda, E., and J. L. Sala. Links Between Terrorism, Organized Crime and Crime: The Case of the Sahel Region. *Stability: International Journal of Security and Development,* Vol. 3, No. 1, Article 27, pp.1-9.

l. Everton, Sean F. *Disrupting Dark Networks.* Cambridge University Press, 2012.

Intentionally Blank

GLOSSARY

ABBREVIATIONS AND ACRONYMS

ABIS	Department of Defense Automated Biometric Identification System
AOR	area of responsibility
ASD(HD&GS)	Assistant Secretary of Defense for Homeland Defense and Global Security
ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives (DOJ)
ATP	Army techniques publication
BEI	biometrics-enabled intelligence
BEWL	biometrics-enabled watch list
BI2R	Biometric Identity Intelligence Resource
BIA	behavioral influences analysis
BICES	Battlefield Information Collection and Exploitation System (NATO)
C2	command and control
CA	civil affairs
CBP	Customs and Border Protection (DHS)
CBRN	chemical, biological, radiological, and nuclear
CCDR	combatant commander
CCIR	commander's critical information requirement
CCMD	combatant command
CEXC	combined explosives exploitation cell
CF	conventional forces
CGTTP	Coast Guard tactics, techniques, and procedures
CI	counterintelligence
C-IED	counter-improvised explosive device
CJCS	Chairman of the Joint Chiefs of Staff
CO	cyberspace operations
COA	course of action
COIN	counterinsurgency
COM	chief of mission
CONOPS	concept of operations
CSA	combat support agency
CT	counterterrorism
CTN	countering threat networks
DATT	defense attaché
DEA	Drug Enforcement Administration (DOJ)
DFBA	Defense Forensics and Biometrics Agency
DFSC	Defense Forensic Science Center
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency

DMDC	Defense Manpower Data Center
DNA	deoxyribonucleic acid
DNI	Director of National Intelligence
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
DODM	Department of Defense manual
DOJ	Department of Justice
DOMEX	document and media exploitation
DOS	Department of State
DRS	detainee reporting system
EA	executive agent
ECP	entry control point
EEFI	essential element of friendly information
EO	executive order
EOD	explosive ordnance disposal
EPW	enemy prisoner of war
EU	European Union
F3EAD	find, fix, finish, exploit, analyze, and disseminate
FBI	Federal Bureau of Investigation (DOJ)
FDO	foreign disclosure officer
FEI	forensic-enabled intelligence
FHA	foreign humanitarian assistance
FID	foreign internal defense
FM	field manual (Army)
FTR	forensics technical representative
FXT	forensic exploitation team
GCC	geographic combatant commander
HD	homeland defense
HN	host nation
HSPD	homeland security Presidential directive
HUMINT	human intelligence
HVI	high-value individual
I2	identity intelligence
I2PO	Identity Intelligence Project Office (DIA)
I2SP	identity intelligence support packet
I2TIP	identity intelligence tracking intelligence package
IC	intelligence community
ICD	intelligence community directive
ICE	Immigration and Customs Enforcement (DHS)

IDENT	Department of Homeland Security Automated Biometric Identification System
IED	improvised explosive device
IGO	intergovernmental organization
IIR	intelligence information report
INTERPOL	International Criminal Police Organization
IO	information operations
IOM	identity operations manager
IPC	interagency policy committee
IW	irregular warfare
J-2	intelligence directorate of a joint staff
J-2E	joint force exploitation staff element
J-3	operations directorate of a joint staff
J-4	logistics directorate of a joint staff
J-5	plans directorate of a joint staff
J-6	communications system directorate of a joint staff
JDEC	joint document exploitation center
JDN	joint doctrine note
JFAIDD	Joint Federal Agencies Intelligence DNA Database
JFC	joint force commander
JIDC	joint interrogation and debriefing center
JIDO	Joint Improvised-Threat Defeat Organization (DTRA)
JIOC	joint intelligence operations center
JIPOE	joint intelligence preparation of the operational environment
JOA	joint operations area
JP	joint publication
JPP	joint planning process
JPRC	joint personnel recovery center
JS	Joint Staff
JTF	joint task force
KLE	key leader engagement
KST	known or suspected terrorist
MCDP	Marine Corps doctrinal publication
MCIP	Marine Corps interim publication
MNF	multinational force
MOC	memorandum of cooperation
MOE	measure of effectiveness
MOP	measure of performance
NAI	named area of interest
NATO	North Atlantic Treaty Organization
NCTC	National Counterterrorism Center

NDIS	National DNA Index System (FBI)
NDP	National Disclosure Policy
NEO	noncombatant evacuation operation
NGI	Next Generation Identification (FBI)
NGO	nongovernmental organization
NMEC	National Media Exploitation Center
NSC	National Security Council
NSPD	national security Presidential directive
NSS	national security strategy
NTTP	Navy tactics, techniques, and procedures
ODNI	Office of the Director of National Intelligence
OE	operational environment
OPE	Office of Partner Engagement (DIA)
OPT	operational planning team
OSD	Office of the Secretary of Defense
OUSD(P)	Office of the Under Secretary of Defense for Policy
PIR	priority intelligence requirement
PN	partner nation
PO	peace operations
PPD	Presidential policy directive
PR	personnel recovery
PSA	principal staff assistant
RFI	request for information
ROE	rules of engagement
RUF	rules for the use of force
SDO	senior defense official
SECAF	Secretary of the Air Force
SECARMY	Secretary of the Army
SecDef	Secretary of Defense
SFA	security force assistance
SIGINT	signals intelligence
SIPRNET	SECRET Internet Protocol Router Network
SJA	staff judge advocate
SOF	special operations forces
SSA	security sector assistance
TCO	transnational criminal organization
TCP	theater campaign plan
TEDAC	Terrorist Explosive Device Analytical Center (FBI)
TF	task force
TIDE	Terrorist Identities Datamart Environment

TSOC	theater special operations command
TTP	tactics, techniques, and procedures
UN	United Nations
USC	United States Code
USCG	United States Coast Guard
USCYBERCOM	United States Cyber Command
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy
USG	United States Government
USSOCOM	United States Special Operations Command
UW	unconventional warfare
VBSS	visit, board, search, and seizure
VEO	violent extremist organization
WMD	weapons of mass destruction


JOINT
CHIEFS OF STAFF