BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 10-701

24 JULY 2019

Operations

OPERATIONS SECURITY (OPSEC)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at: **www.e-Publishing.af.mil** for downloading or ordering

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: AF/A3TY

Certified by: AF/A3TY (Col Schoepf)

Supersedes: AFI10-701, 8 June 2011; AFI10-712, 17 December 2015

Pages: 57

This publication implements Air Force Policy Directive (AFPD) 10-7, *Air Force Information Operations*, Department of Defense Directive 5205.02, *DoD Operations Security (OPSEC) Program*, Department of Defense Manual 5205.02-M, *DoD Operations Security (OPSEC) Manual*. It provides guidance and procedures on operations security (OPSEC) throughout the Air Force (AF). This AFI is consistent with the guidance in Department of Defense Instruction (DoDI) 8560.01, *Communications Security (COMSEC) monitoring and Information Assurance (IA) Readiness Testing* and AFPD 17-1, *Information Dominance Governance and Management*. It applies to individuals at all levels including, the Air Force Reserve (AFR), Air National Guard, civilian and contractor personnel except where noted otherwise. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records* and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). Refer recommended changes and questions about this publication to the Office of Primary Responsibility listed above using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate chain of command. This publication may be supplemented at any level, but all supplements that directly implement this publication must be routed to the Office of Primary Responsibility listed above for coordination prior to certification and approval. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See AFI 33-360, *Publications and Forms Management*, for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of

command to the appropriate Tier waiver approval authority, or alternately, to the requestors commander for non-tiered compliance items.

SUMMARY OF CHANGES

This document is substantially revised and must be completely reviewed. This revision updates the roles and responsibilities for major commands (MAJCOMs), direct report units (DRUs), field operating agencies (FOAs), Air Force Forces (AFFOR), Air and Space Operations Centers (AOC), wings, wing equivalent organizations, OPSEC Program Managers (PM), Signature Managers, Planners and Coordinators. This revision introduces the Air Force OPSEC Support Team (AF OST) and the Cyberspace Defense Analysis Weapon System. It updates guidance related to signature management and the profiling process. Additionally, it introduces OPSEC external assessments (OEA), previously known as OPSEC surveys, OPSEC internal assessments, OPSEC program management assessments and OPSEC reviews; and it incorporates guidance on conducting Electronic System Security Assessments (ESSA), which was previously maintained in AFI 10-712, Cyberspace Defense Analysis and Notice and Consent Operations.

Chapter 1

OPERATIONS SECURITY (OPSEC) OVERVIEW

1.1. National Security Decision Directive 298, *National Operations Security Program* **requires each executive department and agency with a national security mission to have an OPSEC program.** Likewise, DoDD 5205.02E, *DoD Operations Security (OPSEC) Program*, supports the national program and requires each Department of Defense (DoD) component to establish and maintain an OPSEC program.

1.2. OPSEC is an information-related capability that preserves friendly essential secrecy by using a process to identify, control and protect critical information and indicators. If critical information and indicators are disclosed, it could allow adversaries or potential adversaries to identify and exploit friendly vulnerabilities leading to increased risk to mission failure or the loss of life. The desired effect of OPSEC is to influence the adversary's behavior and actions by reducing the adversary's ability to collect and exploit critical information and indicators about friendly activities.

1.3. Essential secrecy is the condition achieved by denying critical information and indicators to adversaries. Adversaries in possession of critical information can hinder or prevent friendly mission accomplishment. Thus, essential secrecy is a prerequisite for effective operations.

1.4. OPSEC, when closely integrated and synchronized with other information-related capabilities, security disciplines and all aspects of protected operations, preserves essential secrecy. OPSEC does this by systematically identifying and managing critical information and indicators attendant to military operations and activities, to deny an adversary the ability to interpret friendly intentions, capabilities, or activities in sufficient time to act effectively against friendly mission accomplishment. It is impossible to avoid all risk and protect everything. Attempting to protect all information diverts resources from actions needed for mission success. Instead organizations should seek an efficient and effective cost solution that balances their risk assessment against vulnerabilities and potential threats to their critical information and indicators.

1.5. OPSEC supports planning, preparation, execution and post execution phases of all activities, operations and programs across the entire spectrum of military operations. Enhanced operational effectiveness occurs when decision-makers apply OPSEC from the earliest stages of planning. Exclusion of OPSEC in the early stages of strategy and operational planning limits the effectiveness of operations and consequently degrades the commander's ability to gain information superiority.

1.6. Commanders and directors are responsible for identifying and managing signatures associated with Air Force activities, capabilities, operations, and programs. Signatures can be managed by implementing and practicing good OPSEC. OPSEC will be integrated into all military functions such as military strategy, command and control, operational and tactical planning and execution, continuity of operations, Air Force specialized training, and military accession. OPSEC shall also be coordinated and integrated into all security disciplines such as cyber, information, industrial, personnel and physical, law enforcement, antiterrorism and force protection. In addition, OPSEC shall be integrated into relevant support activities; contingency; combat and peacetime operations and exercises; communications/computer architectures and processing; critical infrastructure protection; science and technology efforts, weapons systems

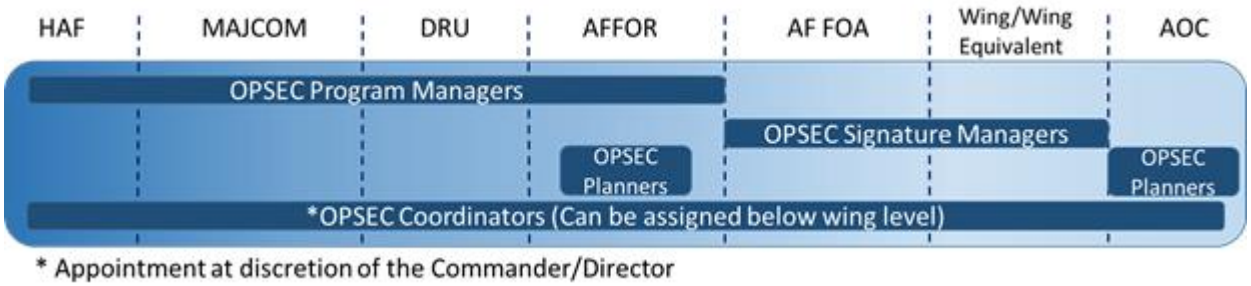
research, development, test and evaluation processes; inspections; acquisition and procurement; and medical operations. **(T-0). Note:** Science and technology efforts and research, development, test and evaluation activities are high-priority targets for collection and are particularly vulnerable to compromise for both classified and unclassified information and have an inherent requirement to implement OPSEC.

1.7. OPSEC is a commander's/director's responsibility and is established, managed and implemented at all levels throughout the AF. It is an operations function and shall be integrated into all operational planning and coordinated with relevant information operations functions. **(T-0).**

1.7.1. To ensure effective implementation across organizational and functional lines of operations, the management of OPSEC should reside in the operations and/or plans element of an organization. For those organizations with no traditional operations or plans element, the commander/director determines the most logical organization to place management and responsibility of their OPSEC program.

1.7.2. The Air Force OPSEC program management structure consists of senior leadership oversight and OPSEC practitioners (program managers, signature managers, coordinators, planners, instructors and OPSEC Support Team members) at appropriate command levels as illustrated in **Figure 1.1**., Air Force Operations Security Organizational Structure.

Figure 1.1. Air Force Operations Security Organizational Structure.



1.7.3. An OPSEC program consists of policies, accountability, mechanisms for enforcement, operating staff, tactics, techniques and procedures, education, training and equipping functions necessary to enable the conduct of OPSEC planning and execution and to ensure the highest level of leadership oversight.

1.8. OPSEC is everyone's responsibility. Air Force personnel at all levels will:

1.8.1. Be familiar with the organization's critical information, indicators and threats. **(T-0).**

1.8.2. Protect critical information and indicators from disclosure. **(T-0).**

1.8.3. Protect all electronic communications containing critical information and indicators. **(T-0).**

1.8.4. Not publicly disseminate, or publish information or imagery displaying critical information such as improvised explosive device strikes, battle scenes, casualties, destroyed or damaged equipment, personnel killed in action (both friendly and adversary) and the protective measures of military facilities or other critical information as identified by the critical information and indicators list within each organization. This prohibition extends to publishing sensitive information via social media and other internet-based capabilities without the appropriate level of oversight and approval. **(T-0).**

1.9. To enhance the effectiveness and understanding of OPSEC: The Air Force provides education and training for all Air Force personnel (e.g., military, Department of the Air Force civilians, DoD Contractors, family members). Additionally, the Air Force conducts internal and external assessments utilizing tools and capabilities such as the AF OST, Electronic Systems Security Assessments (ESSA) and Enterprise Protection Risk Management (EPRM).

1.10. Ideally, the Air Force uses OPSEC countermeasures to protect its critical information. Failure to properly implement countermeasures can result in serious injury or death to Air Force personnel, damage to weapons systems, equipment and facilities, loss of sensitive technologies, and mission degradation or failure.

1.11. Air Force OPSEC SharePoint Sites. The Air Force maintains OPSEC SharePoint sites on both the Non-classified Internet Protocol Router Network and the Secret Internet Protocol Router Network (SIPRNet). Air Force OPSEC practitioners request access to the SharePoint sites through their MAJCOM/DRU OPSEC Program Manager or the AF OST.

1.11.1. The SharePoint site **https://cs2.eis.af.mil/sites/10054/default.aspx** located on the Non-classified Internet Protocol Router Network is the central location for unclassified collaboration of OPSEC. Examples of awareness briefings, training materials, potential communication technology threats and lessons learned are available on the SharePoint site.

1.11.2. The OPSEC SharePoint site located on SIPRNet **https://intelshare.intelink.sgov.gov/sites/signaturemanagement/SitePages/Home.aspx** is the central storage and collaboration space for OPSEC at the SECRET level.

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. Air Force Judge Advocate General (AF/JA).

2.1.1. Provides oversight and guidance on all legal matters pertaining to OPSEC assessments, procedures and activities.

2.1.2. Reviews and provides consultation regarding the use of OPSEC assessment derived information in disciplinary proceedings including courts-martial, non-judicial punishment and adverse administrative proceedings.

2.2. The Deputy Chief of Staff for Manpower, Personnel & Services (AF/A1). Responsible for policy and guidance of manpower, personnel, education, and training support to OPSEC. AF/A1 ensures manpower assessments are conducted to determine appropriate manpower levels to accomplish OPSEC duties across the AF. **(T-0).**

2.3. The Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance (AF/A2). Responsible for policy and guidance of intelligence support to OPSEC by providing integrated, evaluated, analyzed and interpreted information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. Intelligence informs adversary actions, capabilities and intentions. AF/A2:

2.3.1. Provides foreign intelligence collection threat information support to Air Force OPSEC. **(T-0).**

2.3.2. Provides written regional threat assessments in support of OPSEC. When this is not practical or possible, forward requirements through proper channels to the appropriate threat analysis center. Update written threat information as necessary, to include adversary collection means against an organization's current situation and environment.

2.3.3. Provides threat assessments of current, updated and future modification, additions and technical capabilities of collection capabilities regarding Open Skies Treaty observation flights.

2.4. The Deputy Chief of Staff for Operations (AF/A3). Implements DoD and Joint Staff OPSEC policy and establishes OPSEC guidance and procedures, through the Director of Training and Readiness (AF/A3T). Directs the establishment of manpower, funding and resources to implement Air Force OPSEC.

2.4.1. Director of Training and Readiness (AF/A3T). Responsible for the development of Air Force OPSEC policy, programs, guidance, OPSEC support capabilities and activities.

2.4.2. Establishes policy, oversight and resource advocacy for Air Force OPSEC and ESSA operations. **(T-0).**

2.4.3. Appoints a full-time OPSEC Program Manager charged with ensuring the Air Force plans, executes, resources and funds OPSEC consistent with Air Force activities and DoD policy. **(T-0).**

2.4.4. Provides the Deputy under Secretary for Defense (Intelligence) an annual assessment of Air Force OPSEC. **(T-0).**

2.4.5. Ensures threat-based comprehensive OPSEC assessments are conducted across the Air Force every three years to evaluate and assess the effectiveness and efficiency of OPSEC. Identifies, prioritizes, schedules and conducts OPSEC assessments to reduce risk to and enhance mission effectiveness. These assessments may include but are not limited to Air Force weapons systems, research, development, test and evaluation, acquisitions, treaty verification, nonproliferation protocols, international agreements, force protection operations, special access programs, and activities that prepare, sustain, or employ military services over the range of military operations. **(T-0).**

2.4.6. Ensures the risk of exposure to critical information, alone or through the compilation of classified information is mitigated by providing OPSEC training and guidance for those using DoD Internet of Things, other Internet-based capabilities, emerging technologies, or developing information sharing environments accessible across the enterprise. **(T-0).**

2.4.7. Ensures the establishment and management of a capability to conduct ongoing OPSEC and communications security vulnerability analysis on automated information systems or applications and/or programs designed for net-centric interoperability for data aggregation (e.g., component websites, SharePoint sites, email, radios, telephone and other communication systems and methods). **(T-0).**

2.4.8. Ensures the establishment and management of an OPSEC support capability to provide for OPSEC program development, planning, training, assessment, exercise, and operational support to AF activities, functions, missions, organizations and programs. **(T-0).**

2.4.9. Ensure policy and guidance is established and implemented directing deploying personnel to complete OPSEC training specific to their operating area. **(T-0).**

2.4.10. Ensures the establishment of the Air Force OPSEC Working Group. **(T-0).**

2.5. Deputy Chief of Staff, Logistics, Engineering and Force Protection (AF/A4). Ensures OPSEC is implemented to protect the supply chain, design and testing to counter the threat to Air Force operations and activities posed by foreign intelligence collection systems.

2.6. Secretary of the Air Force Office of Information Dominance and Chief Information Officer (SAF/CIO A6).

2.6.1. Ensures OPSEC is included in cybersecurity and cyberspace policy, guidance and operational activities. **(T-0).**

2.6.2. Ensures OPSEC measures and practices are correctly reflected in the Air Force Enterprise Architecture. **(T-0).**

2.6.3. Ensures OPSEC is incorporated into the development of net-centric operating environments to mitigate risks of classification through compilation of critical information and indicators. **(T-0).**

2.6.4. Ensures the Air Force has the capability to monitor, collect and analyze information from DoD electronic communications systems, to determine if any Air Force critical or classified information transmitted via unsecured and unprotected systems could adversely affect US (and allied/coalition) operations and activities. **(T-0).**

2.6.5. Establishes policy and guidance for notice and consent certification and related matters. **(T-0).**

2.7. The Secretary of the Air Force, Office of Public Affairs (SAF/PA).

2.7.1. Coordinates with the Air Force OPSEC Program Office, as required, to ensure appropriate OPSEC content is included in public affairs training and education. **(T-0).**

2.7.2. Ensures policy and procedures are established to ensure OPSEC reviews are accomplished within the Public Affairs Security and Policy Review process and that OPSEC considerations are integrated into information release processes. **(T-0).**

2.7.3. Provides policy and oversight of all content on official Air Force external-facing websites. **(T-0).**

2.7.4. Establishes and maintains on-going collaboration with information security, OPSEC and other relevant stakeholders, as required, to minimize potential OPSEC vulnerabilities while engaging with the public or media.

2.8. The Secretary of the Air Force for Acquisition, Technology & Logistics (SAF/AQ).

2.8.1. Ensures OPSEC is included in program protection plans to protect critical information and indicators throughout the life-cycle of Air Force acquisition and research, development, test and evaluation for critical program information reference AFI 63-101/20-101, *Integrated Life Cycle Management*. **(T-0).**

2.8.2. Ensures acquisition, research, technology and OPSEC functions work together to protect critical information and indicators throughout the Acquisition Integrated Life Cycle framework. **(T-0).**

2.8.3. Ensures individuals who perform acquisition duties receive appropriate OPSEC training in support of program protection planning. **(T-0).**

2.9. The Administrative Assistant to the Secretary of the Air Force (SAF/AA). Provides coordination and integration of OPSEC policy, guidance and procedures within the Air Force security function.

2.10. The Secretary of the Air Force, Inspector General (SAF/IG).

2.10.1. Ensures OPSEC is inspected through the Unit Effectiveness Inspection in accordance with (IAW) AFI 90-201, *The Air Force Inspection System*.

2.10.2. Ensures the Air Force Office of Special Investigations (AFOSI) supports the Commander's or Director's OPSEC responsibilities with counterintelligence activities and criminal investigation information to reduce the risk of adversary exploiting friendly forces critical information and indicators. **(T-0).**

2.10.3. Ensures AFOSI supports the AF OST with counterintelligence activities and criminal investigation information as requested to conduct threat-based comprehensive OPSEC external assessments. This support enhances the AF OST's ability to reproduce the intelligence image in light of the known collection capabilities of potential adversaries against friendly capabilities and intentions.

2.11. The Office of the Secretary of the Air Force General Counsel (SAF/GC).

2.11.1. Provides oversight and guidance on all legal matters pertaining to ESSA procedures and activities.

2.11.2. Reviews and provides consultation regarding the use of ESSA derived information in disciplinary proceedings including courts-martial, non-judicial punishment and adverse administrative proceedings.

2.12. Secretary of the Air Force Chief Data Officer (SAF/CO).

2.12.1. Ensure OPSEC is included in enterprise data management policy, guidance, and operational activities. **(T-0).**

2.12.2. Ensure OPSEC measures and practices are reflected in Air Force Enterprise Data Management activities. **(T-0).**

2.12.3. Ensure the collection of information is properly transmitted and collected according to OPSEC policy and guidance.

2.13. Air Combat Command (ACC). As the lead command for OPSEC will:

2.13.1. Manage OPSEC support within exercises and sourcing of request for forces.

2.13.2. Define and advocate for OPSEC resources.

2.13.3. Perform programming and budgeting for the OPSEC Program Elements.

2.13.4. Manage, develop and implement OPSEC Concept of Operations and tactics, techniques and procedures.

2.13.5. Establish, manage and maintain OPSEC education and training to meet AF, DoD and Joint Staff OPSEC requirements.

2.13.6. Establish and provide travel funding for Air Force OPSEC training to Air Force personnel performing OPSEC duties.

2.13.7. Fund, as necessary, attendance at non-Air Force OPSEC training for Air Force personnel performing OPSEC duties.

2.13.8. Establish, resource, manage and maintain an OPSEC training capability to provide formal OPSEC training to Air Force OPSEC practitioners. The OPSEC training capability must:

2.13.8.1. Provide OPSEC training and mobile training teams as necessary.

2.13.8.2. Identify, train and recommend for certification additional Air Force OPSEC instructors as necessary.

2.13.8.3. Maintain Interagency OPSEC Support Staff adjunct instructor certification and course curriculum currency.

2.13.8.4. Support the development of OPSEC training and education.

2.13.8.5. Support Air Force and DoD-level OPSEC curriculum reviews as requested.

2.13.8.6. Support development of OPSEC policy and guidance for education and training.

2.13.8.7. Manage and provide student training data as necessary.

2.13.8.8. Coordinate with the AF OST regarding OPSEC-related trends obtained from OPSEC assessments and incorporate into OPSEC curriculum.

2.13.8.9. Provide an annual report to Air Force OPSEC Program Manager regarding OPSEC training activities accomplished during the fiscal year. **(T-0).**

2.13.9. Establish, resource, manage and maintain a vulnerability analysis capability to monitor, collect and analyze information traversing or residing on DoD electronic communications systems for OPSEC concerns. **(T-0).**

2.13.9.1. Coordinate and validate current and future monitoring, collection and analyzing requirements, processes and resources with the Air Force OPSEC Program Manager.

2.13.9.2. Ensure ACC/JA provides guidance pertaining to ESSA procedures and activities.

2.13.9.3. Provide annual report to Air Force OPSEC Program Manager regarding OPSEC vulnerability assessment findings and trend analysis. **(T-0).**

2.13.9.4. Ensure ESSA support is provided to the AF OST.

2.13.10. Establish, resource, manage and maintain an effective OPSEC support capability. **(T-0).** The OPSEC support capability will:

2.13.10.1. Manage and provide OPSEC reach-back support (e.g., education, planning, readiness training, assessments and operational support) to all Air Force organizations. **(T-0).**

2.13.10.2. Manage and conduct OPSEC external assessments and OPSEC program management assessments to assist organizations in developing effective OPSEC programs. **(T-0).**

2.13.10.3. Assist in National, DoD, Joint and AF-level OPSEC activities as required.

2.13.10.4. Coordinate with cyberspace defense analysis organizations to receive ESSA products regarding the status of potential OPSEC disclosures discovered during cyberspace defense analysis operations.

2.13.10.5. Coordinate with cyberspace defense analysis organizations and the Information Operations Formal Training Unit regarding trends observed from assessments for inclusion in future ESSA and OPSEC curriculum.

2.13.10.6. Assist in the development of OPSEC continuing education and training of the general Air Force population. **(T-0).**

2.13.10.7. Advise, evaluate and support research and development efforts for OPSEC tools supporting combatant commands. **(T-0).**

2.13.10.8. Ensure AF OST members complete the Air Force OPSEC Course within 90 days of appointment to OPSEC duties as outlined in **chapter 4**. **(T-0).**

2.13.10.9. Ensure AF OST members complete the Defense OPSEC Planners Course within 120 days of appointment to OPSEC duties as outlined in **chapter 4**. **(T-0).**

2.13.10.10. Support the Joint OPSEC Support Element in OPSEC activities as necessary.

2.13.10.11. Manage the Air Force OPSEC SharePoint sites.

2.13.10.12. Assist with the development and documentation of OPSEC related lessons-learned and tactics, techniques and procedures.

2.13.10.13. Provide annual report to Air Force OPSEC Program Manager regarding AF OST functions identified in **paragraph 2.13.10.1**. **(T-0).**

2.14. Air Force Materiel Command. Air Force Materiel Command will integrate OPSEC into all research, development, test and evaluation programs to provide a consistent and effective level of protection throughout the life cycle of all weapon systems and capabilities. **(T-0).**

2.15. Air Education and Training Command (AETC). AETC will:

2.15.1. Ensure OPSEC training is provided in all Air Force accessions (e.g., Basic Military Training School, Reserve Officer Training Corps and Officer Training School). At a minimum, the orientation will include the definition and purpose of OPSEC, threat awareness, vulnerabilities, countermeasures and the individual's role in protecting critical information. **(T-0).**

2.15.2. Incorporate OPSEC education into all professional military education. At a minimum, this will include the purpose of OPSEC, critical information, indicators, threats, vulnerabilities, countermeasures and the individual's role in protecting critical information. **(T-0).**

2.15.3. Incorporate OPSEC concepts and capabilities into an Air Force Continuum of Learning as presented in specialized courses, such as the Contingency Wartime Planning and Joint Air Operations Planning Courses. These courses will include command responsibilities and responsibilities of OPSEC Planners supporting joint planning and execution efforts. **(T-1).**

2.15.4. Establish a validation process in coordination with the Air Force OPSEC Working Group to ensure a content review of all OPSEC training materials within all AETC accession and professional military education.

2.16. Air Force Academy. Will provide OPSEC education for all Air Force Academy accessions. At a minimum, OPSEC education will include the definition and purpose of OPSEC, threat awareness, vulnerabilities, countermeasures and the individual's role in protecting critical information. **(T-0).**

2.17. Commanders/Directors at all levels. The Commander/Director will:

2.17.1. Maintain essential secrecy of the Air Force activities within their enterprise and retain overall responsibility for risk management decisions and the implementation of OPSEC countermeasures. They must understand the risk to the mission and then approve countermeasures for implementation to mitigate said risk. To achieve this end state, commanders/directors will establish, resource and maintain effective OPSEC. **(T-0). Note:** Commanders/Directors may delegate responsibility for the management of OPSEC to a level no lower than the A3 or appropriate Director for MAJCOM/DRU and Vice or Deputy Commander/Director for Centers, Wings, Laboratories and wing-equivalent organizations.

2.17.2. Ensure personnel accomplishing duties as an OPSEC Program Manager, OPSEC Signature Manager, OPSEC Planner, OPSEC Instructor, or OPSEC Support Team Member gain and maintain Top Secret access, are placed in Top Secret manpower billets and are eligible for Sensitive Compartmented Information. **(T-2).**

2.17.3. Ensure OPSEC Program Managers, OPSEC Signature Managers, OPSEC Planners, OPSEC Instructors, and OPSEC Support Team Members establish and maintain a SIPRNet account to have access to classified threat data and OPSEC tasks. **(T-1). Note:** Recommend OPSEC Program Managers, OPSEC Signature Managers, OPSEC Planners, OPSEC Instructors, or OPSEC Support Team members establish and maintain a Joint Worldwide Intelligence Communication System account to access Top Secret-level threat information enhancing the development of effective countermeasures to mitigate risk to operational activities.

2.17.4. Ensure personnel conducting duties as an OPSEC Coordinator gain and maintain a Secret clearance. **(T-2).** Recommend OPSEC Coordinators establish and maintain a SIPRNet account to have access to classified threat data and OPSEC tasks.

2.17.5. Ensure potential OPSEC vulnerabilities are handled IAW the appropriate classification authorities and DoDI O-3600.02, *Information Operations Security Classification Guide*. The DoDI O-3600.02 is located on the DoD Issuance website **https://directives.whs.smil.mil** on the SIPRNet.

2.17.6. Reports of potential OPSEC vulnerabilities will be sent in memorandum format to the MAJCOM or DRU OPSEC Program Manager using the appropriate network based on the classification of the information. **(T-2).**

2.17.7. Ensure procedures are established and implemented to conduct OPSEC reviews of contract documentation prior to public release. **(T-0).**

2.17.8. Ensure, when applicable, OPSEC requirements are properly reflected in government contracts.

2.18. Commanders at MAJCOMs, DRUs and Air Force Forces (AFFOR). Commanders will:

2.18.1. Ensure written guidance is issued to integrate OPSEC into day-to-day and contingency operations. **(T-0).**

2.18.2. Ensure coordination with other command-level organizations. **(T-1).**

2.18.3. Ensure measures are taken to manage signatures, prevent disclosures of critical information and indicators and maintain essential secrecy. **(T-0).**

2.18.4. Ensure critical information and indicators are identified and the risk assessed for each Air Force activity relating to the planning, development, deployment and movement of equipment, personnel, weapon systems and capabilities and document their mitigation efforts, whether the activity is planned, conducted, or supported. **(T-0).**

2.18.5. Appoint in writing a full-time primary and alternate OPSEC Program Manager. **(T-1).**

2.18.5.1. Ensure primary OPSEC Program Managers are appointed at grades no lower than O-4 or GS-13, for MAJCOMs and DRUs and O-3, E-7, or GS-11 for AFFOR Staffs. **(T-2).**

2.18.5.2. Ensure alternate OPSEC Program Managers are appointed at grades no lower than O-2, E-7, or GS-11 for MAJCOMs and DRUs and O-1, E-6, or GS-9 for AFFOR Staff. **(T-2).**

2.18.6. Ensure OPSEC Program Managers are appointed for no less than two-years for the Air Force to optimize their training investment. **(T-2).**

2.18.7. Ensure DoD Contractors are not appointed as primary or alternate OPSEC Program Managers. **Note:** DoD Contractors may be assigned as OPSEC analysts as long as there is government oversight. DoD Contractors may not accomplish inherently governmental functions. Inherently governmental functions are functions that are so intimately related to the public interest as to require performance by Federal Government employees. This means that contractors cannot make decisions that obligate the Federal Government. **(T-0).**

2.18.8. Establish billets for and designate within the command, based on mission requirements, OPSEC Planners at grades no lower than O-3, E-6, or GS-9. **(T-2).**

2.18.9. Appoint OPSEC Coordinators where it makes operational sense in the command's directorates and special staff offices to implement and enhance the effectiveness of the command's OPSEC Program and support the command's OPSEC Program Manager. Contractors may be assigned as an OPSEC Coordinator. **Note:** To reduce potential conflict of interest, prior to awarding a contract requiring a contractor to be an OPSEC Coordinator, consult the local contracting office to ensure there are no inherently governmental functions associated with the OPSEC Coordinator duties. **(T-3).**

2.18.10. Ensure OPSEC concepts are incorporated and institutionalized into relevant strategies, operations, plans, programs, budgets, exercises and training and evaluation methods. **(T-0).**

2.18.11. Ensure intelligence and counterintelligence organizations support the organization's intelligence requirements such as providing classified threat reports, indoctrination to the intelligence activities of the organization and other activities necessary to integrate OPSEC into exercises and operational planning. **(T-0).**

2.18.12. Ensure contracting documents explicitly state the contractor's OPSEC responsibilities and requirements to protect the critical information and indicators associated with the activity, operation or program being contracted. **(T-0).**

2.18.13. Ensure OPSEC Program Managers and Contracting representatives work together when writing requests for proposals, statements of work, performance work statements, statements of objectives or other contract documents to ensure mission critical information and indicators are not placed in unclassified contract documents. **(T-2).**

2.18.14. Ensure OPSEC education and training is provided as referenced in **Chapter 4** for all assigned military, Department of the Air Force civilians and DoD Contractors. **(T-0).**

2.18.15. Ensure OPSEC Working Groups are established. **(T-0).**

2.18.16. Ensure annual internal OPSEC reviews and assessments are conducted as referenced in **Chapter 5**. **(T-1).**

2.18.17. Ensure subordinate organizational commanders/directors provide support as requested during AF OPSEC external assessments. **(T-1).**

2.18.18. Ensure annual OPSEC reviews of organizationally owned, operated or controlled external-facing websites and media sites are conducted to confirm critical information and indicators are not available to the public. **(T-0).**

2.18.19. Ensure OPSEC considerations are included in public affairs security policy review and all other public information release processes. **(T-0).**

2.18.20. Ensure the OPSEC Program Manager, Treaty Compliance Officer and Senior Intelligence Officer, work together to identify and mitigate the risks associated with Open Skies Treaty observation flights. **(T-1).**

2.18.21. Ensure a report detailing OPSEC risk assessment and mitigation efforts on Open Skies Treaty observation activities within the commander's/director's enterprise is completed and made available upon request. **(T-1).**

2.18.22. Ensure an Annual OPSEC Report is completed, signed and forwarded to the appropriate higher headquarters OPSEC Program Manager as referenced in **Chapter 5**. **(T-0).**

2.19. Commanders/Directors at Field Operating Agencies (FOA), Wings and Wing Equivalent Organizations (e.g., Centers, Laboratories). Commanders/Directors will:

2.19.1. Ensure measures are taken to manage signatures, prevent disclosures of critical information and indicators and maintain essential secrecy. **(T-0).**

2.19.2. Ensure coordination with the organization's command-level, other organizations and tenant(s) on the installation to ensure the protection of mission critical activities and capabilities. **(T-0).**

2.19.3. Appoint in writing a primary OPSEC Signature Manager at grades no lower than O-3, E-7 or GS-12 and appoint in writing an alternate OPSEC Signature Manager at grades no lower than O-1, E-6 or GS-9. **(T-2).**

2.19.3.1. Ensure OPSEC Signature Managers are appointed for no less than two-years for the Air Force to optimize their training investment. **(T-3). Note:** Locations where the tour of duty is less than two years are exempt from the 2-year requirement.

2.19.3.2. Ensure DoD Contractors are not appointed as OPSEC Signature Managers. **(T-0).**

2.19.4. Where it makes operational sense, appoint OPSEC Coordinators in the unit's subordinate organizations and on the commander's/director's staff to implement and enhance the effectiveness of OPSEC within the organization and support the organization's OPSEC Signature Manager. Contractors may be assigned as an OPSEC Coordinator.

2.19.5. Organizations requiring contract support for OPSEC related activities must ensure contract requirements do not include the performance of inherently governmental functions and avoid or mitigate personal and organizational conflicts of interest. **(T-0).**

2.19.6. Ensure implementation of command-level OPSEC guidance to incorporate and institutionalize OPSEC concepts into relevant documents and day-to-day and contingency operations. **(T-0).**

2.19.7. Ensure critical information and indicators are identified and the risk assessed for each Air Force activity relating to the planning, development, deployment and movement of equipment, personnel, weapon systems and capabilities and document their mitigation efforts, whether the activity is planned, conducted, or supported. **(T-0)**

2.19.8. Ensure intelligence and counterintelligence organizations support the organization's intelligence requirements such as providing classified threat reports, indoctrination to the intelligence activities of the organization and other activities necessary to integrate OPSEC into exercises and operational planning. **(T-0).**

2.19.9. Ensure annual OPSEC reviews and internal assessments are conducted. **(T-2).**

2.19.10. Ensure required support is provided to the AF OPSEC Support Team as requested during AF OPSEC external assessments. **(T-1).**

2.19.11. Ensure annual OPSEC reviews of organizationally owned, operated or controlled external-facing media sites are being conducted to confirm critical information and indicators are not being made available to the public. **(T-0).**

2.19.12. Ensure OPSEC considerations are included in Public Affairs Security Policy Review and all other public information release processes. **(T-0).**

2.19.13. Ensure OPSEC education and training is provided as referenced in **Chapter 4** for all assigned personnel (military, Department of the Air Force civilians and DoD Contractors). **(T-0).**

2.19.14. Ensure contracting documents explicitly state contractor OPSEC responsibilities and requirements to protect critical information and indicators for the contracted activity, operation, or program. **(T-0).**

2.19.15. Ensure contract requirement owners coordinate with OPSEC Signature Managers, the contracting office and other stakeholders to ensure mission critical information and indicators are not placed in publicly available contract documents. **(T-1).**

2.19.16. Ensure OPSEC Working Groups are established as required and integrated with similar protection/security related working groups. **(T-3).**

2.19.17. Ensure the OPSEC Signature Manager, Treaty Compliance Officer and Senior Intelligence Officer, work together to identify and mitigate the risks associated with Open Skies Treaty observation flights. **(T-1).**

2.19.18. Ensure an Annual OPSEC Report is completed, signed and forwarded to the appropriate higher headquarters OPSEC Program Manager as referenced in **Chapter 5**. **(T-0).**

2.20. Air Force OPSEC Program Manager is the appointed adviser to Air Force Leadership regarding Air Force OPSEC. The Air Force OPSEC Program Manager will:

2.20.1. Develop, communicate and ensure implementation of standards, policies and procedures to protect the essential secrecy of Air Force activities, operations and programs. **(T-0).**

2.20.2. Identify requirements and necessary resources for the effective implementation of OPSEC. **(T-0).**

2.20.3. Review and assess the effectiveness and efficiency of Air Force OPSEC. **(T-0).**

2.20.4. Within 90 days of appointment, complete the required OPSEC IAW **Chapter 4**. **(T-0).**

2.20.5. Identify, prioritize and request OPSEC assessments and provide oversight and advocacy as the focal point for Air Force OPSEC assessment capabilities. **(T-0).**

2.20.6. Participate in DoD and National OPSEC training and education reviews to identify DoD and Federal OPSEC training requirements. **(T-0).**

2.20.7. Chair the Air Force OPSEC Working Group. **(T-0).**

2.21. OPSEC Program Managers at MAJCOMs, DRUs and AFFORs. OPSEC Program Managers will:

2.21.1. Serve as the commander's/director's representative regarding OPSEC requirements and the point of contact for all OPSEC-related issues between the Air Force OPSEC Program Manager, AF OST and the organization's subordinate units. **(T-1).**

2.21.2. Maintain responsibility for OPSEC inherently governmental functions. **(T-1).**

2.21.3. Advise the commander/director on the identification and protection of the organization's critical information and indicators. **(T-1).**

2.21.4. Establish, maintain, review and confirm at least annually, the currency of the organization's critical information and indicators list and countermeasures. **(T-0).**

2.21.5. Annually, review and assess the effectiveness and efficiency of OPSEC within the organization, to include currency and effectiveness of subordinate organization's procedures to control critical information and indicators. **(T-0).**

2.21.6. Participate in budget development activities to identify manpower, funding and resources to effectively implement and sustain the OPSEC program. **(T-0).**

2.21.7. Develop and monitor OPSEC program expenditures. **(T-0).**

2.21.8. Develop, implement, distribute and annually review the commander's OPSEC guidance and procedures. **(T-0).**

2.21.9. Advise the commander/director on the placement of OPSEC Coordinators where they will have an operational impact in supporting the MAJCOM/DRU and AFFOR OPSEC Program. **(T-0).**

2.21.10. De-conflict implementation of OPSEC countermeasures with other MAJCOMs, DRUs, and FOAs. **(T-0).**

2.21.11. Provide oversight, guidance and training to subordinate OPSEC practitioners and working group members as referenced in **Chapter 4**. Training shall include specific roles and responsibilities associated with the assigned OPSEC functions. **(T-0).**

2.21.12. Ensure all other OPSEC education and training is provided as referenced in **Chapter 4**. **(T-0).**

2.21.13. Ensure unit specific OPSEC education materials are provided to organizations which require contract support within 30 days of award of a contract as referenced in **Chapter 8**. **(T-0).**

2.21.14. Within 90 days of appointment, complete the required OPSEC training as referenced in **Chapter 4**. **(T-0).**

2.21.15. Chair the OPSEC Working Group. **(T-0).**

2.21.16. Establish and maintain Command-level OPSEC SharePoint websites. **(T-2).**

2.21.17. Establish and maintain an Enterprise Protection Risk Management user account. **(T-1).**

2.21.18. Review and provide advice on the development of OPSEC Plans. **(T-0).**

2.21.19. Conduct Staff Assistance Visits as requested by subordinate units for OPSEC planning and assistance in operationalizing OPSEC. **(T-2).**

2.21.20. Manage the command's AF OST and ESSA support requirements. **(T-1).**

2.21.20.1. Request ESSA Focused Look Assessments through Twenty-Fourth Air Force (Air Force Cyber) as referenced in **Chapter 5**. **(T-1).**

2.21.20.2. Review ESSA products, determine levels of risk, assess impact and update countermeasures to affected activities as required. **(T-0).**

2.21.20.3. Ensure OPSEC education is provided to prevent reoccurrence of OPSEC disclosures. **(T-0).**

2.21.21. Review applicable contract documents to ensure critical information and indicators are not included in publicly available contract documents. **(T-0).**

2.21.22. Review after-action reports and lessons learned to determine how they apply to the mission and applicability for inclusion into future OPSEC courseware and the Air Force lessons learned database, as prescribed IAW AFI 90-1601, *Air Force Lessons Learned Program*. **(T-1).**

2.22. OPSEC Signature Managers at FOAs, Wings, and wing equivalent organizations' (e.g. Centers, Laboratories). OPSEC Signature Managers will:

2.22.1. Serve as the commander's/director's representative regarding OPSEC requirements and the point of contact for all OPSEC-related issues between their MAJCOM/DRU and AFFOR OPSEC Program Managers and the organization's subordinate units. **(T-2).**

2.22.2. Maintain responsibility for OPSEC inherently governmental functions. **(T-0).**

2.22.3. Advise the commander/director on the identification and protection of the organization's critical information and indicators. **(T-3).**

2.22.4. Identify manpower, funding and resource requirements to the applicable AF/MAJCOM/DRU OPSEC Program Manager. If applicable, develop and monitor OPSEC program expenditures. **(T-2).**

2.22.5. Advise the commander/director on the placement of OPSEC Coordinators where they will have an operational impact in supporting OPSEC. **(T-3).**

2.22.6. Within 90 days of appointment (365 days for traditional Guard and Reserve), complete the required OPSEC training as referenced in **Chapter 4**. **(T-2).**

2.22.7. Provide OPSEC education materials as referenced in **Chapter 4**. **(T-0).**

2.22.8. Establish, maintain, review and confirm at least annually, the currency of the organization's critical information and indicators list and countermeasures. **(T-2).**

2.22.9. Annually, review and assess the effectiveness and efficiency of OPSEC within the organization, to include currency and effectiveness of subordinate organization's procedures to control critical information and associated indicators. **(T-0).**

2.22.10. Ensure planning documents are reviewed annually and update as referenced in **Chapter 7**. **(T-2).**

2.22.11. Develop and integrate OPSEC into all plans to include operational, deployment and exercise plans. **(T-2).**

2.22.12. Coordinate with contract requirement owners to review contract documents to ensure publicly available contract documents do not included unit critical information and indicators. **(T-3).**

2.22.13. Ensure contract requirements explicitly state contractor OPSEC responsibilities and requirements to protect critical information and indicators for the activity, operation or program being contracted. **(T-3).**

2.22.14. Provide unit specific OPSEC education materials to organizations which require contract support within 30 days of award of a contract as referenced in **Chapter 8**. **(T-3).**

2.22.15. Obtain and maintain an EPRM user account. **(T-2).**

2.22.16. Act as the focal point for requesting ESSA and AF OST support through the MAJCOM/DRU OPSEC Program Manager. **(T-2). Note:** FOAs may request ESSA and AF OST support directly to the Twenty-Fourth Air Force (AF Cyber) and AF OST**.**

2.22.17. Submit after-action reports and lessons learned for incorporation into future OPSEC courseware and the Air Force lessons learned database when applicable, as prescribed IAW AFI 90- 1601, *Air Force Lessons Learned Program*.

2.23. OPSEC Planners. OPSEC Planners will:

2.23.1. Within 90 days of appointment, complete the Air Force OPSEC Course as outlined in **Chapter 4**. **(T-0).**

2.23.2. Within 120 days of appointment, complete the Defense OPSEC Planners Course as outlined in **Chapter 4**. **(T-1).**

2.23.3. Integrate OPSEC into the planning process using AF, DoD, and Joint standards, policies, procedures and this instruction as guidance. **(T-0).**

2.23.4. Review annually, operational planning documents and update where necessary. **(T-0).**

2.23.5. Identify critical information and indicators for each air component plan your unit is responsible for implementing. **(T-0).**

2.23.6. Identify current threats that have a capability and intent to obtain and exploit the critical information within the air component plan. **(T-0).**

2.23.7. Identify signatures and indicators related to the movement of equipment, personnel and weapon systems that are directly supporting the air component plan. **(T-0).**

2.23.8. Using the threat analysis and vulnerability analysis of available signature and indicators, conduct a risk assessment associated with the identified vulnerabilities. **(T-0).**

2.23.9. Identify and ensure the integration of OPSEC measures and countermeasures into the plan to reduce vulnerabilities and indicators. **(T-0).**

2.23.10. Coordinate the integration of OPSEC measures and countermeasures with other information-related capabilities. **(T-0).**

2.23.11. Coordinate with other OPSEC Planners regarding OPSEC measures and countermeasures during events and/or operations that may cross over into another regions activities. **(T-2).**

2.24. OPSEC Coordinators at all levels. OPSEC Coordinators will:

2.24.1. Assist in developing and recommending guidance and implementing countermeasures to mitigate the risk of potential adversary exploitation of critical information and indicators. **(T-0).**

2.24.2. Distribute the commander's/director's OPSEC guidance (e.g., critical information and indicators list, memorandums, standard operating procedures, OPSEC Implementation Plans) as required. **(T-3).**

2.24.3. Within 90 days of appointment, complete the required OPSEC training outlined in **Chapter 4**. **(T-0).**

2.24.4. Assist in reviewing and updating OPSEC guidance and procedures for currency. **(T-3).**

2.24.5. Provide unit personnel OPSEC education as referenced in **Chapter 4**. **(T-3).**

2.24.6. Conduct OPSEC reviews of organizational documents and photographs in coordination with Public Affairs prior to public release, as required. **(T-3).**

2.24.7. Assist in reviewing contracting documents to ensure unit critical information and indicators are not publically available in solicitations and other contract documents, as required. **(T-3).**

2.25. Responsible Contracting Office. Contracting Offices will:

2.25.1. Coordinate with contract requirement owners and OPSEC practitioners to identify OPSEC requirements for the work to be performed, as appropriate. **(T-1).**

2.25.2. Incorporate identified OPSEC measures into solicitations and contracts, as appropriate. **(T-0).**

2.25.3. Enforce contract requirements related to OPSEC. **(T-3).**

2.25.4. Assist in the review of contract documents to ensure unit critical information and indicators are not publically available in solicitations or other contract documents. **(T-3).**

Chapter 3

OPSEC PROCESS

3.1. General. The OPSEC process is a systematic method used to identify, control and protect critical information as established in National Security Decision Directive 298. This chapter presents the five elements of the OPSEC process: 1) Identify critical information, 2) Analyze threats, 3) Analyze vulnerabilities, 4) Assess risk and 5) Apply countermeasures. These elements may or may not be used in sequential order but all elements must be present to conduct an OPSEC analysis. When planning in a contingency or crisis dynamic situation elements may need to be revisited at any time. The Air Force uses OPSEC to enhance mission effectiveness by managing signatures. Additionally, a profiling process is employed to identify and understand how the use of specific information systems and conduits to accomplish operational missions and activities. Within the AF, process-related subject matter experts are consulted to create the most accurate list of critical information, the identification of vulnerabilities and indicators allowing us to conduct a thorough risk analysis. This risk analysis provides Air Force leadership with options, based on the risk analysis results to manage signatures to protect Air Force activities.

3.2. Identify Critical Information:

3.2.1. Critical information includes specific facts about friendly activities, intentions, capabilities, or limitations that an adversary seeks to gain a military, diplomatic, economic, or technological advantage. Such information, if revealed to an adversary may prevent or degrade mission accomplishment, cause loss of life or damage friendly resources. This step only identifies potential critical information items. The resulting critical information and indicators list should not be published as the unit's official critical information and indicators list until the remainder of the OPSEC process is completed. Other steps within the OPSEC process may remove, refine, or add additional items from/to the list.

3.2.2. The identification of critical information is a key part of the OPSEC process because it focuses the remainder of the OPSEC process on protecting vital information rather than attempting to protect all unclassified information. The individuals responsible for the planning and execution of the organization's mission are the ones that can best identify their critical information. Additionally, using an adversarial approach and asking what information an adversary wants to know about the mission is a helpful method when trying to identify critical information.

3.2.3. Once the OPSEC process is completed, compile the critical information and indicators identified into a critical information and indicators list, obtain the commander/director approval and disseminate it to all organizational personnel to ensure they are aware of the information which requires protection.

3.2.4. Identify critical information at the earliest stages of planning an operation or activity and continuously update as necessary to support mission effectiveness.

3.2.5. Strive to keep critical information and indicators list unclassified "For Official Use Only". Critical information and indicators lists assist to remind personnel to protect related critical information and indicators. Do not release critical information and indicator list to the public.

3.3. Analyze Threats:

3.3.1. A threat is an adversary with the capability and intent to undertake action detrimental to mission success, to include associated program activities and/or operations. An adversary is any entity with goals counter to your own.

3.3.2. Threat information is necessary to understand what to protect and subsequently develop appropriate countermeasures. Analyzing threats includes identifying potential adversaries and their associated capabilities and intentions to collect, analyze and exploit critical information and indicators.

3.3.3. Analyzing threat involves the research and analysis of intelligence, counterintelligence and open-source information to identify the likely adversaries to the planned operation. The operation planners, working with the intelligence and counterintelligence staffs, assisted by the OPSEC Practitioner, will seek answers to the following threat questions:

3.3.3.1. Who is the adversary? (Who has the intent and capability to take action against the mission? Who are the friends of these adversaries? Who are the Air Force's potential adversaries?).

3.3.3.2. What are the adversary's intentions and goals? (What does the adversary want to accomplish?).

3.3.3.3. What are the adversary's intelligence collection capabilities (e.g., Human Intelligence, Imagery Intelligence, Signals Intelligence, Measurement and Signature Intelligence, Open-source Intelligence)?

3.3.3.4. What are the adversary's tactics (courses of action) for opposing the mission? (What actions might the adversary take?).

3.3.3.5. What critical information or indicators does the adversary already know about the operation? (What information is it too late to protect?).

3.3.3.6. What is the adversary's methodology for collecting on friendly forces?

3.3.4. Intelligence organizations provide tailored intelligence threat information in support of the Commander's Priority Intelligence Requirements. AFOSI provides counterintelligence threat information that includes but is not limited to foreign intelligence services, foreign and domestic terrorist organizations, criminals, cyber-based threats, lone extremists groups, economic competitors. Reports from cyberspace organizations can be used to assess cyber threats and vulnerabilities.

3.4. Analyze Vulnerabilities:

3.4.1. A vulnerability exists when the adversary is capable of collecting critical information and/or indicators, correctly analyzing them and acting quickly enough to impact friendly objectives.

3.4.2. An adversary exploits vulnerabilities to obtain critical information. The adversary then uses the information collected to support their decision-making process thus obtaining an operational advantage. The vulnerability can be in an organization's procedures, a failure of traditional security, poor judgment on the part of leadership, lack of threat awareness, the use of unsecure information systems without encryption to process critical information or the system design itself. Conducting exercises and analyzing operations can help identify vulnerabilities.

3.4.3. An indicator is a friendly detectable action and/or open-source information that can be interpreted or pieced together by an adversary to derive critical information. All indicators have characteristics making them identifiable or causing them to standout. The characteristics of an indicator are: signatures, profiles, associations, contrast and exposure.

3.4.4. A vulnerability analysis is the examination of your processes, projects or missions to determine if you have inherent, naturally occurring or self-induced vulnerabilities or indicators that put your critical information and thus your mission at risk.

3.5. Assess Risk:

3.5.1. Risk is a measure of the potential degree to which critical information is subject to loss through adversary exploitation. The assessment of risk evaluates the degree of probable harm or adverse impact that a vulnerability or combination of vulnerabilities may cause if exploited by an adversary. It involves assessing the adversary's ability to exploit vulnerabilities that would lead to the exposure of critical information and the potential impact it would have on the mission. Determining the level of risk is a key element of the OPSEC process and provides justification for the use of countermeasures. Conduct risk assessments and develop recommended countermeasures based on operational planning and the current operating environment. A typical risk assessment will:

3.5.1.1. Determine the level of risk by comparing the vulnerabilities identified with the probability of an adversary being able to exploit those vulnerabilities and the impact if exploited.

3.5.1.2. Once the amount of risk is determined, identify potential countermeasures to reduce the vulnerabilities with the highest risk. The most desirable countermeasures are those combining the highest possible protection with the least amount of resource requirements and/or adverse effects on mission goals.

3.5.1.3. Consider the cost, time and effort of implementing measures and countermeasures to mitigate risk. Factors to consider include:

3.5.1.3.1. What are the benefits of the proposed countermeasures to reduce risks compared to the negative effects on the mission?"

3.5.1.3.2. What is the cost of the proposed countermeasure compared with the cost associated with the impact if the adversary exploits the vulnerability?

3.5.1.3.3. Will implementing the countermeasure create a new OPSEC indicator?

3.6. Apply Countermeasures:

3.6.1. Countermeasures are anything which negates or reduces an adversary's ability to exploit Air Force vulnerabilities. Countermeasures are designed to prevent an adversary from detecting critical information, provide an alternative interpretation of critical information or indicators (deception), or deny the adversary the ability to utilize their collection system to exploit Air Force operations. Countermeasures may be offensive or defensive in nature (e.g., camouflage, concealment, deception, intentional deviations from normal patterns, direct strikes against adversary collection capabilities). If the commander/director determines the risk level is unacceptable, implement countermeasures to mitigate the risk and reduce it to an acceptable level.

3.6.2. The OPSEC Working Group submits recommended countermeasures for commander/director approval.

3.6.3. Countermeasures must be synchronized and integrated with other information-related capabilities to achieve synergies in efforts to influence the adversary's perceptions and situational awareness.

3.6.4. Countermeasures must be coordinated with other affected organizations to ensure they do not become vulnerabilities or unacceptable indicators.

3.6.5. During the execution of countermeasures, monitor the adversary's reaction, if possible, to provide feedback that can be used to assess effectiveness or determine potential unintended consequences.

3.7. Signature Management. Commanders defend or exploit operational profiles through the management of signatures. This is accomplished by identifying processes and details within an Air Force activity to map and understand their operational profiles. Signature management is the active defense or exploitation of operational profiles resident at a given military installation or organization.

3.7.1. Defense of operational profiles is accomplished by implementing countermeasures to deny or mitigate adversary collection of critical information.

3.7.2. Using a profiling process allows the commander to define the local operating environment and captures process points that present key signatures and profiles with critical information value. This process is the deliberate effort to identify functional area process and the observables they produce to contribute to the overall signature of day-to-day activities and operational trends. Once completed, the results can be used to develop execution checklists, critical information and indicators list and identify key process points for potential protection or exploitation. This ultimately provides commanders several options to exploit or deny signatures to enhance mission effectiveness.

Chapter 4

OPSEC EDUCATION AND TRAINING

4.1. General. All Air Force personnel (military, Department of the Air Force Civilians and DoD Contractors) require a general knowledge of threats, vulnerabilities, countermeasures and their responsibilities associated with protecting critical information. OPSEC education is a continuous requirement. All personnel require OPSEC awareness education within 60 days of their accession into the Air Force, prior to any deployment and when required by the commander/director. **(T-0).**

4.2. OPSEC Awareness Education:

4.2.1. Air Force OPSEC education provides an overview of the OPSEC process, the definition of OPSEC, its purpose, what is critical information, the individual's role in protecting critical information and the general adversary threat to the AF's critical information.

4.2.2. The Air Force OPSEC Program Manager provides standardized baseline OPSEC education materials to the MAJCOM, DRU and FOA for distribution within each of their organizations.

4.2.2.1. Commanders/Directors may use this standardized material to provide localized OPSEC education via commander's call, training days, or similar events.

4.2.2.2. OPSEC education must include, at a minimum, updated threat information, changes to critical information and indicators, new procedures and/or OPSEC measures implemented, altered or deleted by the organization. **(T-0).**

4.2.2.3. OPSEC Program Managers and Signature Managers are responsible for developing OPSEC education to reduce risk to the commander's/directors mission priorities. **(T-0).**

4.2.2.4. The circulation of directives, memos for record, posters, or similar material on a "read and initial" basis shall not be utilized as a sole means of fulfilling any of the specific requirements of OPSEC education. **(T-0).**

4.2.2.5. OPSEC Signature Managers record the completion of OPSEC Education through locally developed means and include information in the annual OPSEC report. **(T-2).**

4.2.3. DoD Contractors with OPSEC requirements within a contract must ensure employees receive OPSEC training as specified in the contract. Accomplishment of training must not exceed 90 days from initial assignment to a contract with OPSEC requirements. Access to mission critical information will not be allowed until OPSEC education has been completed and documented. **(T-0).**

4.2.4. Procurement of low-cost promotional items and awareness aids (e.g., pens, pencils, magnets, key chains, lanyards) are authorized for the exclusive intent to promote and reinforce OPSEC education in accordance with organizational missions. For guidance, refer to AFI 65-601, Vol 1, *Budget Guidance and Procedures*.

4.3. Mission-Oriented OPSEC Awareness Education:

4.3.1. Mission-oriented OPSEC education is event-driven and ensures all affected Air Force personnel are familiar with potential threats related to the organization, critical information for the mission it supports, job specific OPSEC indicators and the OPSEC measures unique to that specific event.

4.3.2. Mission-oriented OPSEC education includes, at a minimum, updated threat information, changes to critical information and indicator list, new procedures, and/or OPSEC measures implemented, altered or deleted by the organization. **(T-0).**

4.3.3. Mission-oriented OPSEC education may be directed by the commander/director to address specific events not covered by annual OPSEC education such as personally identifiable information breaches, change of mission, updates to the critical information and indicator list, recurring OPSEC disclosures, new threats and/or vulnerabilities, countermeasures.

4.3.4. OPSEC Pre-Deployment Awareness Education: Prior to their departure, obtain and provide deploying personnel OPSEC awareness of critical information and indicators pertaining to their deployed location. **(T-0).** Theater-specific critical information and indicators that require protection can be obtained from the deployed location's OPSEC Program Manager or OPSEC Signature Manager.

4.4. Air Force OPSEC Training. Air Force OPSEC training is funded by the Air Force lead command for OPSEC (HQ ACC). Non-Air Force OPSEC training is funded at the unit level. MAJCOM/DRU OPSEC program managers may request HQ ACC funding to attend non-Air Force OPSEC training by forwarding a Memorandum for Record for funding via an official email to the HQ ACC OPSEC program manager. The requests must include a justification why current Air Force OPSEC training cannot meet the organization's operational requirements. Organizations will be required to fund non-Air Force OPSEC training if funding is not available or current Air Force OPSEC training is available and sufficient to meet operational requirements. If training requirements are not completed within 180 days, OPSEC Program Managers must report training deficiencies through the Defense Readiness Reporting System with a get-well date. The frequency of completing the following courses is one-time. **(T-0).** (See **Table 4.1**, Air Force OPSEC Training Requirements, within this instruction for applicable training courses).

4.4.1. Air Force OPSEC Course. The Air Force OPSEC Course is required for all Air Force OPSEC Program Managers, OPSEC Signature Managers, OPSEC Instructors, Air Force OST members, OPSEC Planners and Information Operations Officers (Air Force Specialty 14F). The Air Force OPSEC Course is required to be completed within 90 days of appointment to OPSEC duties. **(T-0).** It is especially useful and should be attended by Military Deception Program Managers/Planners, or others deemed necessary by MAJCOMs/DRUs. MAJCOM OPSEC program managers are responsible for nominating personnel from their subordinate organizations to HQ ACC to attend the Air Force OPSEC Course. The Air Force OPSEC program manager is responsible for nominating personnel from DRU and FOAs to HQ ACC to attend the Air Force OPSEC Course. The Air Force OPSEC Course is required to be completed within 90 days of appointment to OPSEC duties.

4.4.1.1. The Air Force OPSEC Course educates students on how to identify observable activities and operational trends that reveal critical information and indicators to potential adversaries. The course provides training on how to develop and maintain an OPSEC program and hands-on activities and instruction on how to incorporate OPSEC tactics, techniques and procedures across the range of military operations. This training postures Air Force organizations to plan and execute flexible and adaptive activities, while protecting our own information, in support of higher headquarters and commander's objectives/effects.

4.4.1.2. Air Force and MAJCOM OPSEC Program Managers are responsible for identifying personnel within their organizations that are eligible for TDY funding to the Air Force OPSEC Course.

4.4.1.3. Individuals who have completed the Air Force OPSEC Course are not required to complete the Air Force Identity Management computer-based training. (See **paragraph 4.4.4**.)

4.4.1.4. If scheduling conflicts exist, the MAJCOM/DRU OPSEC Program Manager must document and ensure the OPSEC practitioner is scheduled for the next available course not to exceed 180 days. If training is not completed within 180 days, OPSEC Program Managers must report training deficiencies through the Defense Readiness Reporting System with a get-well date. **(T-0).**

4.4.2. Defense OPSEC Planners Course (DOPC). The Defense OPSEC Planners Course provides OPSEC Planners and AF OST members training to effectively plan, integrate, conduct and assess OPSEC at the joint/operational level, across the range of military operations. The Defense OPSEC Planners Course, taught by the Joint OPSEC Support Element, is the accepted Air Force level course for OPSEC Planners. The Defense OPSEC Planners Course is mandatory for Air Force OPSEC planners and AF OST members. **(T-0).** MAJCOM and DRU OPSEC program managers are responsible for nominating personnel within their subordinate organizations to the Joint OPSEC Support Element to attend the Defense OPSEC Planners Course. For mandatory attendees, the course is required to be completed within 90 days of appointment to OPSEC duties. **(T-0)**. Though OPSEC Program Managers and OPSEC Signature Managers are not required to attend the DOPC, they may attend using unit funding.

4.4.3. OPSEC Fundamentals. The OPSE-1301, OPSEC Fundamentals course is mandatory for all Air Force OPSEC program managers, OPSEC signature managers, OPSEC instructors, AF OST members, OPSEC planners, OPSEC coordinators and Information Operations Officers (Air Force Specialty 14F). The course is found on the Advanced Distance Learning Service **https://golearn.adls.af.mil/login.aspx** and the Interagency OPSEC Support Staff **https://www.iad.gov/ioss** websites. It is the prerequisite course to attend all formal OPSEC training courses. The course is required to be completed within 30 days of appointment to OPSEC duties. The OPSEC Fundamentals training provides basic information about OPSEC. The course focuses on the history of OPSEC, the OPSEC process described in National Security Decision Directive 298 and provides students with the opportunity to practice OPSEC in a modern scenario. **(T-0).**

4.4.4. Air Force Identity Management Course. The Air Force Identity Management course is mandatory for OPSEC practitioners and public affairs representatives. **(T-0).** It may be of interest to anyone who uses internet-based capabilities. The course is required to be completed within 90 days of appointment to OPSEC and public affairs duties. The Air Force Identity Management course is located on the Joint Knowledge Online website **https://jkodirect.jten.mil/Atlas2/page/login/Login.jsf.** This training introduces the student to common threats, vulnerabilities and countermeasures associated with internet-based capabilities. It provides digital identity education for military members, government employees and DoD Contractors. The course provides an overview of identity management, how to protect your digital identity, discusses various ways outsiders obtain your personally identifiable information and provides recommended OPSEC measures.

4.4.5. OPSEC Contract Requirements. The Continuous Learning Center (CLC) 107 course "OPSEC Contract Requirements" is located on the Defense Acquisition University website **https://www.dau.mil/**. The course introduces the basic elements of OPSEC, identifies the role of OPSEC within DoD and recognizes the OPSEC responsibilities of program managers and Contracting representatives for establishing contracting services. This course is mandatory for OPSEC practitioners and contracting representatives who review contracts. **(T-0).**

4.4.6. Intelligence Oversight. Intelligence oversight training is required for OPSEC Program Managers, Signature Managers, Planners, and AF OST members. **(T-0).** Training materials are available from the MAJCOM Intelligence Oversight Manager. Additional, information regarding intelligence oversight training is available within AFI 14-104, *Oversight of Intelligence Activities*.

Table 4.1. Air Force OPSEC Training Requirements.

TRAINING	OPSEC PPROGRAM MANAGER	OPSEC SIGNATURE MANAGER	OPSEC PLANNER	OPSEC COORD	AF OST MEMBER	AF OPSEC INSTRUCTOR	PUBLIC AFFAIRS	WEBSITE ADMIN	CONTRACTING	INSPECTION TEAM (OPSEC Rep)	TRAINING LOCATION
OPSE 1301 OPSEC Fundamentals	X	X	X	X	X	X	X	X	X	X	ADLS
AF OPSEC Course	X	X	X		X	X	O			O	In-residence Hurlburt Field, Florida
J3O P-US1322, AF Identity Mgmt.	X	X	X	X	X	X	X	X	X		Joint Knowledge Online
CLC-107, OPSEC Contract Requirements	X	X	O	O	X	X			X		Defense Acquisition University website
Defense OPSEC Planners Course	O	O	X		X	O					Provided by Joint OPSEC Support Element via MTT
Intelligence Oversight	X	X	X	O	X	O					AF OPSEC SharePoint Site

O = Optional
X = Required

Chapter 5

EVALUATING OPSEC

5.1. Overview. OPSEC evaluations fall into two categories: OPSEC reviews and OPSEC assessments. OPSEC reviews are methods to determine an organization's compliance with established OPSEC standards or measures of performance. OPSEC assessments are methods to determine the effectiveness of policies, practices, procedures and OPSEC measures to protect an organization's critical information and indicators or measures of effectiveness. In addition, OPSEC assessments may be used during exercises or real-world operations to determine the effectiveness of measures and countermeasures designed to affect adversary collection sensors. **Table 5.1** provides information regarding Air Force OPSEC reviews and assessments.

Table 5.1. OPSEC Reviews and Assessments.

TYPE OF ASSESSMENT	FREQUENCY	CONDUCTED BY	PURPOSE
OPSEC Review	Annually	Each Organization	Examine measures of performance and verify policies or procedures are in place
OPSEC Internal Assessment	Annually and as needed to support sensitive operations, when evidence of adversary efforts to collect critical information or prior to the development of an OPSEC program	Each Organization's Internal Resources	Evaluate the organization's activities & supporting functions to determine if sufficient countermeasures are in place
OPSEC External Assessment (OEA)	As tasked by HAF or requested by MAJCOM, DRU or FOA	AF OST	Pinpoint weaknesses an adversary could utilize to degrade Air Force operations and activities by identifying critical information, indicators & vulnerabilities
OPSEC Program Management Assessment (PMA)	As requested by HAF, MAJCOM, DRU or FOA	AF OST	Determine effectiveness of how OPSEC is managed, implemented, executed and supported within an organization
Electronic Systems Security Assessment (ESSA)	As requested by HAF, MAJCOM, DRU or FOA	AF Cyberspace Defense Analysis Organizations	Determine if any critical or classified information transmitted via electronic communications could adversely affect US (and allied/coalition) operations
Staff Assistance Visit (SAV)	As Needed	OPSEC PM, IG, or other organization SMEs	Program compliance, assisting, repairing and managing OPSEC programs
Website Content Vulnerability Analysis	Annually	OPSEC PM or other OPSEC trained personnel	Ensure critical information is not available for exploitation by potential adversaries on external-facing websites

5.2. OPSEC Reviews. Conducted annually, by the organization to verify policies and procedures are in place and measures of performance are documented and executed to protect critical information and indicators. Results from a review may provide indications of the need for an OPSEC assessment.

5.2.1. Organizations may utilize assessment tools such as the management internal control toolset (MICT), the OPSEC module in the enterprise protection risk management (EPRM) system or staff assistance visits to conduct annual OPSEC reviews.

5.2.1.1. Management Internal Control Toolset. MICT is the Air Force program of record to communicate a unit's program health using self-assessment communicators and special interest item compliance. The Air Force OPSEC self-assessment communicators are developed and managed by the Air Force OPSEC Program Manager. See AFI 90-201, for specific MICT information.

5.2.1.2. Enterprise Protection Risk Management. EPRM's OPSEC Module is a web-based tool developed to provide a standardized process to assist the OPSEC community with assessing and quantifying risk to critical information. This assessment allow informed decisions on what countermeasures to implement to reduce the organization's overall risk and vulnerabilities. EPRM provides posture, vulnerabilities and risk level status, which can provide assistance in developing plans and management reports. It provides a platform for planners to test remediation options and scenarios and provides an expert knowledge base to assist in threat assessments. OPSEC practitioners can request an EPRM account by going to the EPRM site on SIPRNet.

5.2.1.3. Staff Assistance Visit. OPSEC Program Managers, or other organization subject matter experts conduct staff assistance visits as needed in accordance with (IAW) AFI 90-201 and this instruction. The purpose is to assist organizations with managing and implementing OPSEC into plans, repairing dormant, non-compliant, deficient programs. Organizations may request staff assistance visits IAW AFI 90-201. Staff assistance visits check for program compliance (e.g., Special Interest Items, AFIs, MAJCOM policies), identify and resolve shortfalls and provide guidance as required.

5.2.2. OPSEC reviews evaluate:

5.2.2.1. Personnel's knowledge of critical information, indicators and publication of the critical information and indicators list.

5.2.2.2. Personnel's knowledge of the collection threat to the organization and the countermeasures in place to protect against the collection.

5.2.2.3. The implementation of OPSEC countermeasures to protect identified critical information and indicators.

5.2.2.4. Status of OPSEC training within the organization.

5.2.3. Annual OPSEC Report. Annually, each DoD Component is required to submit to the Under Secretary of Defense (Intelligence) an assessment of OPSEC within the component. An annual OPSEC report is completed and submitted by each MAJCOM, DRU, FOA, wing and wing equivalent organization. The annual report shows how well OPSEC is being implemented and practiced in the Air Force. Additionally, the report identifies best practices, gaps and issues within each organization. The identification of gaps and issues enables the Air Force to focus its efforts to remedy those gaps. The annual OPSEC Report is develop by combining fiscal year data from OPSEC program reviews, measures of performance, measures of effectiveness, exercise after-action reports, lessons learned, Unit Effectiveness Inspections and annually conducted external and internal assessments. The report has been assigned Report Control Symbol (RCS) DD-INTEL(A) 2228. **(T-0).**

5.2.3.1. The Air Force OPSEC Program Manager provides Air Force OPSEC Report guidance to the MAJCOMs, DRUs and FOAs.

5.2.3.2. MAJCOMs, DRUs and FOAs are responsible for tasking their subordinate organizations to complete and submit an annual OPSEC report that allows each MAJCOM, DRU and FOA to consolidate and provide a command view of their OPSEC program via the OPSEC report.

5.2.3.3. The MAJCOM, DRU and FOA Commander/Director, or the delegated authority responsible for the organizations OPSEC program signs that organization's Annual OPSEC Report and forwards to the tasking organization.

5.2.3.4. The commander/director or designated representative for organizations below the MAJCOM/DRU signs that organization's Annual OPSEC Program Report and forwards it to their higher headquarters OPSEC Program Manager.

5.3. Assessments. OPSEC assessments are conducted to determine if adequate procedures are in place to protect critical information and indicators and to gauge the overall effectiveness of countermeasures. OPSEC assessments, are conducted annually or when operations or commanders/directors dictate, to evaluate measures of effectiveness of an organization's ability to maintain essential secrecy. The assessment of OPSEC identifies the effectiveness through the evaluation of unit established measures of performance and measures of effectiveness within plans and programs. Measures of performance indicate whether a particular action was performed and measures of effectiveness measure if implemented measures and countermeasures work.

5.3.1. Website Assessment. At least annually, organizations that maintain external-facing web sites conduct content vulnerability analysis of the information on those sites to ensure critical information is not available for exploitation by potential adversaries. External-facing website owners should participate in conducting the annual assessments. They have the best understanding of the scope, intent, and focus of the site and with assistance from an OPSEC Practitioner and a critical information and indicators list can determine if critical information and indicators are present on the site. **Note:** Websites that require a DoD Common Access Card are exempt from this annual requirement.

5.3.2. OPSEC Internal Assessments. An OPSEC Internal Assessment is an overall evaluation of the organization's ability to effectively protect its critical information and indicators. Use the organization's internal assets to conduct internal assessments. The purpose of an internal assessment is to evaluate an organization's activities and supporting functions to determine if sufficient countermeasures are in place to protect against the loss of critical information and indicators.

5.3.2.1. Internal assessments are conducted annually. Additionally, conduct assessments when there is a need to evaluate based on the sensitivity of the operation or activity, or when there is evidence that an adversary is attempting to gain critical information and indicators. These assessments can include deploying OPSEC practitioners to forward operating locations to support assessment of deployed units.

5.3.2.2. Conduct an internal assessment prior to the development of an OPSEC program. The internal assessment can establish an OPSEC profile by revealing indicators that present vulnerabilities for an adversary to exploit. This allows the program to be developed with fact-based knowledge of threats and vulnerabilities that must be addressed.

5.3.3. Electronic Systems Security Assessment (ESSA). Cyberspace Defense Analysis weapon system units conduct ESSAs on Air Force owned, operated, and/or leased communication systems to support OPSEC protection measures. ESSA assists commanders in evaluating their organization's OPSEC posture by identifying the amount and type of information available to adversary collection entities. Commanders may submit request for ESSAs to the 68th Network Warfare Squadron. Once the ESSA request is received, the request will be prioritized based on the type of mission the requesting organization is conducting or supporting. See **paragraph 6.4**., for ESSA request priorities. ESSA monitoring can be tasked and focused on specific information pertaining to Air Force Core Functions, weapon systems, operations, and activities. Awareness of active electronic monitoring of government telecommunication systems is an essential element of deterrence of such disclosures. The monitoring of Air Force communication systems can only be conducted within certain legal parameters and may only be performed by authorized personnel.

5.3.3.1. The Air Force currently monitors three major mediums, which if exploited by adversaries, can negatively affect Air Force operations. Note: Specific capabilities may vary as technology changes.

5.3.3.1.1. Telephony, the monitoring and assessment of Air Force unclassified voice networks.

5.3.3.1.2. Email Communications, the monitoring and assessment of unclassified Air Force email traffic on the Air Force Information Network.

5.3.3.1.3. Radio Frequency Communications, the monitoring and assessment of Air Force communications within radio frequency bands (e.g., mobile phones, land mobile radios, wireless local area networks).

5.3.3.2. ESSA Team Support. OPSEC Program Managers, OPSEC Planners, FOA OPSEC Signature Managers, and members of the AF OST request ESSA support through Twenty-Fourth Air Force (AF Cyber).

5.3.3.3. Guidance regarding ESSA operations is provided in **Chapter 6**.

5.3.3.4. The most effective assessments involve active participation from the assessed unit. This includes clearly describing areas to be assessed, developing quality lists of critical information for which to monitor, and providing feedback on assessment products.

5.3.3.5. Most monitoring activities are provided at no cost to the assessed organization. However, if the assessed organizations require a mode of monitoring that requires physical proximity or request an in-person mission out-brief, the requesting organization must fund the travel of the team conducting the assessment. Additionally, for an on-site assessment, the requesting organization must:

5.3.3.5.1. Coordinate a work area and secure storage facility for the team performing the ESSA mission.

5.3.3.5.2. Assist the team with arrangements for billeting, transportation, and messing.

5.3.3.5.3. Provide necessary technical information when requested, such as frequencies, system specifications, circuit listings, and critical nodes.

5.3.3.5.4. Ensure administrative communication capabilities are available to teams for operational or administrative support. Arrange specialized communications support as needed to meet mission requirements.

5.3.4. OPSEC External Assessment. The AF OST conducts OPSEC external assessments to provide Air Force leadership with an in-depth analysis and feedback on the effectiveness of countermeasures put in place to mitigate adversarial exploitation of Air Force activities and operations. An OPSEC external assessment is not a programmatic assessment. It is a detailed, third-party analysis of Air Force activities and operations associated with a specific Air Force weapon system, core function, or operational event by employing the known collection capabilities of potential adversaries.

5.3.4.1. The OPSEC external assessment requires a team of experts to assess an activity from an adversary’s perspective to determine if critical information and indicators are disclosed through normal operations and functions, to identify vulnerabilities and propose countermeasures to mitigate the disclosure of essential secrets.

5.3.4.2. The primary focus is to identify critical information, indicators and vulnerabilities associated with the operations of the assessed Air Force capability, pinpoint weaknesses an adversary could utilize to degrade Air Force operations and activities and provide Air Force Senior Leadership information about when, where and how a potential adversary could interpret Air Force intentions.

5.3.4.3. OPSEC external assessments determine if current OPSEC countermeasures are effectively mitigating identified threats and vulnerabilities. OPSEC external assessment, recommendations for new or additional countermeasures against existing or future capabilities are identified to better protect assets and increase the operational advantage over adversaries and competitors.

5.3.4.4. The AF OST coordinates their presence at locations with MAJCOM IG Gatekeepers and MAJCOM/DRU OPSEC Program Managers to ensure minimal impact by the team within a commander's enterprise IAW AFI 90-201.

5.3.4.5. To maintain team and mission integrity, it is imperative OPSEC external assessment team members be billeted together, when possible. The OPSEC External Assessment Mission Director, while maintaining requirements established in the Joint Travel Regulations, is responsible for determining appropriate lodging for OPSEC External Assessment team members.

5.3.4.6. The AF OST nominates Air Force OPSEC external assessment targets annually, based on adversary threat information, through the lead MAJCOM to the Air Force OPSEC Program Manager to gain approval of future OPSEC external assessment focus area(s). OPSEC external assessments are comprehensive and potentially multi-site assessments that attempt to collect and exploit Air Force critical information and indicators with the ultimate goal of improving essential secrecy.

5.3.4.7. Results from Air Force OPSEC external assessments are provided in a formalized report to the AF/A3 by the end of February following the completion of the tasked assessment.

5.3.4.8. MAJCOMs, DRUs and FOAs may request an OPSEC external assessment as needed, but OPSEC external assessments must be focused on a specific operation, mission, activity, or capability to allow the AF OST to provide the best results to the organizations.

5.3.4.9. The AF OST forwards results from the MAJCOM, DRU and FOA OPSEC external assessment to the command that requested the assessment. MAJCOMs, DRUs and FOAs should provide an analysis of the results from any OPSEC external assessments conducted for their organizations in their Annual OPSEC Report.

5.3.5. OPSEC Program Management Assessment. An OPSEC program management assessment is a thorough analysis of how OPSEC is implemented, executed, supported and managed to determine the effectiveness of OPSEC within the organization. OPSEC program management assessments are conducted by the AF OST.

5.3.5.1. During an OPSEC program management assessment, the AF OST will work with the assessed organization to identify opportunities to develop and implement more effective methods to enable the improved protection of critical information and indicators.

5.3.5.2. OPSEC program management assessments require considerably more time and effort from the assessed organization's leadership, program managers and general work force than what is required for an OPSEC external assessment. To be successful, the AF OST's activities during an OPSEC program management assessment require dedicated time and resources of the assessed organization to thoroughly understand and assess the OPSEC program.

5.3.5.3. OPSEC program management assessments can be initiated by the assessed organization and/or the organization's higher headquarters. Organizations may request an OPSEC program management assessment as needed, but the program management assessment must be focused on a specific operation, mission, activity, or capability to allow the AF OST to provide the best results.

5.3.5.4. The requesting organization is responsible for coordinating with the MAJCOM and Wing Gatekeepers of the AF OST presence on the installation.

5.3.5.5. The requesting organization is responsible for funding OPSEC program management assessments, unless preapproved by the Director, AF OST.

5.3.5.6. Results from OPSEC program management assessment are included in the AF OST's annual report to the Air Force OPSEC Program Manager. These results provide OPSEC vulnerability trends and allow for the development of effective protective measures.

5.3.5.7. AF/MAJCOM/DRU OPSEC Program Managers and FOA OPSEC Signature Managers are the focal point for requesting and scheduling all external assessments and setting all priorities between command organizations.

5.4. Air Force OPSEC Support Team. The AF OST is the "operational arm" of Air Force OPSEC. The AF OST conducts OPSEC assessments and provides "reach back" support to Air Force units worldwide to include support to OPSEC program development, planning efforts, development of protection methods and development and availability of OPSEC education materials. The AF OST is responsible for:

5.4.1. Program Development: Provides support at the strategic through tactical level in the development of an OPSEC program. Such as support to build and maintain an OPSEC program, development of an OPSEC Implementation Plan and/or provide knowledge and experience (helpdesk type function).

5.4.2. Planning: Provides support at the strategic through tactical level through the development and maintenance of operational plans. This support may include support in areas such as building and maintaining an OPSEC operational planning capability, provide framework of a plan annex, development of countermeasures and mitigation methods, provide knowledge and experience (helpdesk type function) and assist in the development of OPSEC scenarios emulating real world operations, exercises and activities.

5.4.3. Awareness Education: AF OST provides assistance in the development and continued education and training of the Air Force population. This support may include developing and maintaining OPSEC education and training and providing subject matter expertise in the development of education and training materials. The AF OST may also provide, as requested, an OPSEC booth for conferences and other events to help increase OPSEC awareness.

5.4.4. OPSEC Reviews and Assessments: Provide support at the operational and tactical level through the assessment of Air Force OPSEC. This support may include areas such as advice on tools and capabilities, recommend corrective actions, develop capability to conduct program assessments, orchestrate and conduct Air Force OPSEC External Assessments, Air Force OPSEC program management assessments, analyze and evaluate results of assessments and integrate lessons learned.

5.4.5. Open-source Research. Provides open-source research and analysis of new and existing OPSEC vulnerabilities impacting the ability to protect Air Force critical information and indicators. The results from the open-source research and analysis includes recommendations for effective countermeasures to mitigate these vulnerabilities.

Chapter 6

ELECTRONIC SYSTEM SECURITY ASSESSMENT (ESSA)

6.1. Overview. The Air Force employs electronic communications systems such as telephones, cellular phones, radios, pagers, computers, computer networks, internet-based capabilities such as blogs, web-sites, social networking sites and other wired or wireless electronic devices to conduct day-to-day official business. Adversaries can easily monitor these systems to gather information regarding military capabilities, limitations, intentions, and activities. ESSAs provide commanders/directors the type and amount of information traversing DoD electronic communication systems that is at risk to adversary collection and exploitation. Assessments can be used to evaluate personnel compliance with information, personnel, and industrial security practices, communications security and cybersecurity procedures, the implementation and effectiveness of information operations, information warfare and military deception activities and the identification of potential OPSEC vulnerabilities. They are also used to support other security operations, activities, and programs to enhance force protection and focus training requirements.

6.2. Purpose.

6.2.1. The Air Force monitors, collects, and analyzes information from Air Force electronic communications systems to determine if any critical or classified information transmitted via unsecured means could adversely affect US (and allied/coalition) operations.

6.2.2. The use of ESSAs are an integral part of Air Force OPSEC, Information Operations, and Red Teaming. An ESSA is an effective tool to help assess the effectiveness of OPSEC and identify data disclosures that can adversely affect the DoD's ability to maintain essential secrecy.

6.2.3. An ESSA identifies information content transmitted across DoD electronic communication systems in order to assess an organization's OPSEC and network security posture and determine the amount and type of information available to adversary collection entities.

6.3. Monitoring Authority.

6.3.1. The authority to monitor Air Force networks is derived from the Federal Information Security Modernization Act 44, USC 3554. Additional authority and/or legal restrictions may apply based on the specific intent and purpose for the monitoring.

6.3.2. The Cyberspace Defense Analysis Weapon System is the only Air Force capability authorized to conduct ESSA activities. Cyberspace Defense Analysis operators accomplish these activities within specific legal parameters utilizing authorized tools to monitor, collect, and transfer telecommunication data for analysis. They perform ESSA activities in a manner that satisfies the legitimate needs of the Air Force to provide OPSEC assessments while protecting the legal rights and civil liberties of those persons whose communications are subject to communications monitoring.

6.3.3. Monitoring resources can be adjusted during exercises, crises, contingencies, and conflicts. The monitoring and subsequent analysis of data are designed to thoroughly examine communication system procedures associated with a specific weapons system, operation, or activity (focused assessment), and document their vulnerability to hostile intelligence collection and exploitation. These assessments are also conducted to provide information and data into the OPSEC risk analysis process, gauge the overall effectiveness of an activity, program, or operation, and to support Information Operation/Information Warfare objectives.

6.4. ESSA Request Priorities. ESSA missions are prioritized as follows:

6.4.1. Priority 1: Military operations:

6.4.1.1. Priority 1A: Major operations and campaigns

6.4.1.2. Priority 1B: Special operations

6.4.1.3. Priority 1C: Peace operations, crisis response or limited contingency operations

6.4.2. Priority 2: Special access programs or research, development, test and evaluation activities, and OPSEC Assessments:

6.4.2.1. Priority 2A: Existing special access programs

6.4.2.2. Priority 2B: OPSEC External and Program Management Assessments

6.4.2.3. Priority 2C: Test and evaluations

6.4.2.4. Priority 2D: Research and development

6.4.3. Priority 3: Air Expeditionary Force pre-deployment exercises or events

6.4.4. Priority 4: Air Force organizations participating in Joint Chiefs of Staff directed exercises

6.4.5. Priority 5: Combatant command, MAJCOM, HDRU, or HFOA exercises

6.4.6. Priority 6: Baseline assessments

6.4.7. Priority 7: All other assessments

6.5. Release of Monitoring Information. Cyberspace Defense Analysis operators may release identifying information as provided in this section. In all other cases, information that could reasonably identify individuals in assessed offices, flights, or sections, such as titles, names, ranks, complete phone numbers, complete e-mail addresses will not be released to customers. Office symbols may be released if the release of the office symbol does not provide sufficient data to identify an individual. As long as the information in a product does not identify specific individuals as the source of the disclosure, a product may contain names, titles, or ranks when it is an integral part of the possible disclosure.

6.5.1. Adverse or Disciplinary Personnel Actions. Information obtained during an ESSA mission will not be used as evidence in a criminal prosecution without approval of SAF/GC. **(T-0).**

6.5.2. Emergency Situations. If information threatening death, serious bodily harm, significant or intentional compromise of classified information, or major loss of property is obtained during an ESSA:

6.5.2.1. Immediately report this information, as appropriate, to the military commander, AFOSI, U. S. law enforcement agency having jurisdiction of the effected organization, or other agency as necessary to resolve the emergency.

6.5.2.2. Use the most expeditious means of reporting that provides full security.

6.5.2.3. Complete identifying data may be released.

6.5.2.4. Until properly reported, the emergency situation has priority. Resources may be re-assigned and other assessment missions may be suspended or delayed as necessary.

6.5.2.5. Although derived from ESSA activity, emergency information is not included in any ESSA product.

6.5.2.6. Notify, via email, ACC/JA within 24-hours of initial reporting.

6.5.3. Criminal, Foreign Intelligence, and Counterintelligence Information. Information incidentally acquired during ESSA activities that directly relates to criminal, foreign intelligence, and counterintelligence information is reported as follows:

6.5.3.1. Immediately report this information to the unit commander and AFOSI.

6.5.3.2. Complete identifying data may be released.

6.5.3.3. Although derived from ESSA activity, this data is not included in any ESSA product.

6.5.3.4. Notify, via email, ACC/JA within 24-hours of initial reporting. ACC/JA provides a legal review of the report and forwards via command Judge Advocate General Channels to AF/JA and SAF/GC.

6.5.4. Classified Information. If information revealing a compromise or continuing threat of a compromise of classified information is obtained during the assessment, follow the reporting guidance within AFI 16-1404, *Air Force Information Security Program*. If found within an assessed communication:

6.5.4.1. Release only the minimum amount of data necessary to ensure prompt remedial action. Within the report briefly summarize the information that was sent and its classification.

6.5.4.2. If an attachment is present, it may also be sent using secure means to the appropriate information protection office, MAJCOM/DRU OPSEC Program Manager for evaluation. The information protection office is the first level of management for classified information.

6.5.4.3. Release pertinent information to the appropriate commander, network control officials, information protection office, or MAJCOM/DRU OPSEC Program Manager to facilitate the positive identification, containment, and remediation of disclosed data. Pertinent information may include full header information (to, from and cc lines or sending/receiving addresses; dates/times; and subject line) or account information (enclave, username or hostname, password and /or identity certificate).

6.5.5. Distinguished Visitor Movements. If encountered during an assessment, properly report the distinguished visitor movement information IAW AFI 71-101, Volume 2, *Protective Service Matters*, and include this information in an ESSA product.

6.5.5.1. Report high-level distinguished visitor movements, such as the President, Vice President, and foreign heads of state or foreign ambassadors. Report data pertaining to specific dangerous situations and/or a threat, plan, or attempt to physically harm or kidnap certain individuals, as described in AFI 71-101V2. Report this information to the local AFOSI detachment of the ESSA operation, who in-turn reports this information to the local AFOSI detachment at the assessed location.

6.5.5.2. Derivatively classify products utilizing the applicable security classification guide or source document. Specific itineraries may carry a higher classification based on trip sensitivity. For information regarding classification guides contact your local information protection office.

6.5.6. Vulnerabilities to Government Owned/Leased Networks and/or Databases. If vulnerabilities to government owned or leased networks or databases are discovered in the course of an ESSA, release pertinent information to the appropriate commander, network control officials, information protection office, or MAJCOM/DRU OPSEC Program Manager to facilitate the positive identification, containment, and remediation of disclosed data. See **paragraph 6.5.4.3** for a list of pertinent information that may be released. Vulnerabilities are defined as a release of user credentials of government owned or operated systems, network topology data, compromises of personally identifiable information, or other information that may allow an adversary to attack or exploit Air Force networks. **Exception:** Communications to and from various help desks or Cybersecurity offices to report and resolve network or systems issues are not reported.

6.5.7. Breach of personally identifiable information. Breaches of personally identifiable information must be reported as directed in AFI 33-332, *Air Force Privacy Program and Civil Liberties Program*. A reportable personally identifiable information breach is defined as "actual or possible loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic." In such cases, report the names of all parties who committed the potential breach, the facts, and the circumstances around the potential breach to the servicing Air Force Installation and Mission Support Center Privacy Act Program Manager and associated MAJCOM/DRU OPSEC Program Manager.

6.6. ESSA Products. All ESSA products are marked and protected at a minimum FOR OFFICIAL USE ONLY until possible disclosures are thoroughly evaluated and any weaknesses corrected. ESSA products are classified and marked according to DoD Instruction O-3600.02, *Information Operations (IO) Security Classification Guidance*, DoDM 5200.01, Volume 4, *DoD Information Security Program: Controlled Unclassified Information (CUI)* and current policy and guidance. Prior to marking classified documents individuals should be trained IAW AFI 16-1404 and DoDM 5200.01, Volume 3, *DoD Information Security Program: Protection of Classified Information.*

6.6.1. Types of ESSA Products. There are two basic types of ESSA products, reports and transcripts.

6.6.1.1. Reports. ESSA reports provide operational commanders with awareness of critical information or through compilation classified information disclosures that may adversely affect U.S. (and allied/coalition) operations. Commanders should use these reports for evaluating the effectiveness of OPSEC countermeasures and developing measures to diminish the value of disclosed information. ESSA reports include information protection alerts, immediate, trend, and summary reports. ESSA reports are provided to all organizations effected whether the ESSA is a part of continuous monitoring or a focused assessment. ESSA products are sent to those organizations that are impacted by the information disclosed, data loss, or vulnerability trend. At a minimum, a copy of all sanitized ESSA products will be sent to the higher headquarters OPSEC Program Manager of all the affected organizations and the AF OST when the disclosing organization is scheduled for an OPSEC external assessment.

6.6.1.1.1. An Information Protection Alert is a shortened reporting format used to notify the customer of possible disclosures upon discovery during an ongoing assessment. These alerts may contain information of value to foreign intelligence collection services, unclassified critical information, or information pertaining to the movement of high level distinguished visitors.

6.6.1.1.2. Immediate reports provide time-critical information, force protection information, compromises of classified information, and/or mission critical information during exercise and real-world operations.

6.6.1.1.3. Trend reports are issued whenever analysis uncovers a significant trend of damage and/or vulnerabilities. These reports may summarize and analyze damage and/or vulnerabilities covered in previous ESSA reports or OPSEC indicators in aggregate that uncover larger vulnerabilities. Trend reports may be labeled as ESSA, but may contain information from ESSA-derived information as well as, non-ESSA-derived sources.

6.6.1.1.4. Summary reports are used to review all information gathered following a completed organization requested ESSA. The summary report reviews all information put at risk or disclosed and all information in aggregate used during the risk and damage assessments. This report is typically issued within 60-calendar days of completion of the assessment. Summary reports may be labeled as ESSA, but may contain information from ESSA-derived information as well as, non-ESSA-derived sources.

6.6.1.2. ESSA Transcripts. There are two types of transcripts, sanitized and un-sanitized. A transcript can be part or all of a verbatim reproduction of an assessed communication and may include certain identifying information (sanitized versus un-sanitized). It may also contain transcriber's comments or remarks to clarify or enhance understanding of the information presented. All transcripts (sanitized or un-sanitized) are classified according to content. All markings for both classified and unclassified transcripts must be IAW DoD Instruction O-3600.02, *Information Operations (IO) Security Classification Guidance*, DoDM 5200.01, Volume 2, *DoD Information Security Program: Marking of Information* and DoDM 5200.01, Volume 4, *Information Security Program: Control Unclassified Information (CUI)*. **(T-0).**

6.6.1.2.1. Sanitized transcripts are furnished upon request of an organization. A sanitized transcript is a true representation of a communication but will not contain personally identifiable information. Sanitized transcripts may be requested by the higher headquarters OPSEC Program Manager of the affected organization and the AF OST when the disclosing organization is scheduled for an OPSEC external assessment.

6.6.1.2.2. Un-sanitized transcripts are true and complete representation of a communication(s). Un-sanitized transcript may be attached to or included in other reports to streamline notifications when possible. An organization may request an un-sanitized transcript. An un-sanitized transcript includes both the sending and receiving communicator's information (if available). Un-sanitized transcripts may be requested by the higher headquarters OPSEC Program Manager of the affected organization.

6.7. Active Indicator Monitoring Products. Active Indicator Monitoring products are used to report network vulnerabilities and personally identifiable information disclosures, as described in sections 6.5.6. and 6.5.7.

6.7.1. A personally identifiable information report may be generated when identifying information specific to an individual has been sent unencrypted from or to an Air Force Information Network account. Cyberspace Defense Analysis units will not retain personally identifiable information after reporting procedures have been accomplished, except as required to support compliance with Federal laws and Air Force guidance or for formal training purposes.

6.7.2. A Network Vulnerability Report is generated when monitoring reveals the disclosure of information that may result in the compromise of government networks or systems. A Network Vulnerability Credential Report identifies the disclosure of individual or group credentials for a government account or system. A Network Vulnerability Baseline Report identifies the disclosure of a listing of hardware or software details for an Air Force system or network. A Network Vulnerability Topology Report identifies the disclosure of the topological structure of an Air Force network, such as in network diagrams.

6.8. Other Products. Cyberspace Operations Risk Assessment reports analyze the impact of potential and confirmed disclosures of data from adversary exfiltration. Cyberspace Operations Risk Assessment applies OPSEC principles and processes in the conduct of responsive and systematic analysis of the content and impact of disclosed data leaving the Air Force Information Network. Authorities for Cyberspace Operations Risk Assessment missions are derived from AFI 17-201, *Command and Control (C2) for Cyberspace Operations*. Other products may be generated as needed to meet disclosure release requirements.

Chapter 7

OPSEC PLANNING

7.1. General. This chapter provides direction for planners to integrate OPSEC into operational plans.

7.1.1. The continuous planning, implementation and assessment of countermeasures throughout military operations enhance a commander's ability to shape the information environment, achieve desired effects and meet operational objectives. The basic principles, capabilities and activities of OPSEC planning remain the same whether units are at home station or deployed—only the specific focus of the planning process changes. OPSEC provides systematic and comprehensive analysis designed to identify and manage observable friendly actions that could portray intentions and/or capabilities and is most effective when integrated with other information related capabilities as part of the strategy development, planning and execution phases of operations.

7.1.2. OPSEC planning efforts may result in formal portions of an operational planning document (i.e., Tab C to Appendix 3 to Annex C of an operational plan) or a separate OPSEC Plan (also referred to as a Signature Management Plan) that focuses on a small-scale, limited event requiring specific, additional OPSEC countermeasures (i.e., the silent movement of aircraft overseas). Examples of OPSEC planning products are available from the AF OST.

7.1.3. Proper OPSEC planning ensures that sensitivities of friendly operations are identified, vulnerabilities to the hostile intelligence collection and exploitation are assessed and protective measures are identified and executed.

7.2. Incorporating OPSEC into Operational Planning. Operational planning is typically focused at the AFFOR and/or AOC, with reach-back support outside the theater when appropriate. When planning duties are split, all responsible entities integrate OPSEC into their planning efforts (see also Joint Publication 3-13.3, *Operations Security*, Chapter 3). When there is no Component-MAJCOM, as the supported organization, the theater AOC resolves debates and provides general guidance. OPSEC Planners are the focal point for integrating OPSEC into the operational planning function using skills and processes learned in the Defense OPSEC Planners Course or equivalent course.

7.2.1. OPSEC planning and subsequent executed countermeasures focus on protecting the operation's overall essential secrets as defined by the Combatant Command or Joint Task Force Commander and their designated planning staff. OPSEC Planners consider the standardized operational aspects of presence, capability, strength, intent, readiness, timing, location and method to identify appropriate essential secrets. Analysis results of the five-part OPSEC process translate specifically to the seven steps of the Joint Planning Process.

7.2.2. OPSEC will be included in all operation plans, concept plans and operation orders, etc. Planners will use established tactics, techniques and procedures to develop Tab C to Appendix 3 to Annex C to the operation order or operational plan. The planning staff will identify critical information and indicators from all functional areas requiring protection throughout each phase of the operation. Use risk assessments to identify applicable countermeasures to mitigate any unacceptable operational risks. Develop measures of performance and measures of effectiveness for each OPSEC countermeasure. Review plans annually and update as needed.

Consider changes in the threat, vulnerabilities, impact to the plan and measures of effectiveness and measures of performance of implemented countermeasures.

7.2.3. Component headquarters will include in their OPSEC Plans the Critical Information and Indicators List, threats, vulnerabilities, countermeasures and points of contact for supporting organizations (e.g. wings/wing-equivalents deploying for exercises, operations and/or systems under development and sustainment). This action will occur as soon as the organization(s) are identified so that critical information and indicators can be protected before there are compromises to operations or system acquisitions. Classify OPSEC Plans IAW respective security classification guidance.

7.2.4. OPSEC Program Managers, OPSEC Signature Managers and/or OPSEC Coordinators assist organizational planners and OPSEC Planners to incorporate protection of critical information and indicators into supported operational plans, concept plans and supporting plans.

7.3. Incorporating OPSEC into Support Plans. Along with wartime operational plans, OPSEC will be integrated into all support plans (e.g., programming plans and in-garrison expeditionary site plans). **Note:** See AFI 10-404, *Base Support and Expeditionary Site Planning*, for Base Support Plan requirements and format.

7.4. Incorporating OPSEC into Exercise Planning. To enhance a unit's combat readiness and improve crisis response capabilities units should include OPSEC into their exercise plans. OPSEC Planners should identify specific training objectives for the exercise and achieve the objectives using OPSEC-focused scenarios to assist the training audience and exercise control group during the training event. Incorporate specific OPSEC scenarios into the exercise's Master Scenario Events Listings, along with specific measures of performance and measures of effectiveness to assess the proficiency of Commanders to mitigate loss of critical information and indicators as well as validating personnel's ability to execute countermeasures. OPSEC Planners should plan and implement OPSEC countermeasures for exercises to minimize observations of sensitive training activities by adversary surveillance and treaty verification activities.

7.4.1. For wing level exercises, OPSEC Signature Managers, OPSEC Planners and OPSEC Coordinators assist Wing Inspection Team members and exercise planners in developing Master Scenario Events Listings and measures of performance to train organization personnel in the application or execution of countermeasures.

7.4.2. For exercises higher than the wing level, OPSEC Program Managers, OPSEC Planners, OPSEC subject matter experts within the exercise control group that develop OPSEC scenarios and implementers that directly reflect the exercised unit's missions and operations as tasked in applicable concept plans, executive orders and/or operational plans. Scenarios and implementers must measure impact to operations and mission success if OPSEC is not implemented. Track Master Scenario Events Listing injects in Joint Training Information Management System from start to completion in order to validate a units' ability to complete OPSEC Mission Essential Task and rate the unit with T (Trained), P (Partially Trained), U (Untrained). Joint Training Information Management System provides visibility to wing and above unit training status, allows exercised units to define yearly training requirements and provides training objectives for future exercises.

7.4.3. Evaluators submit deficiencies or best practices to the MAJCOM OPSEC Program Manager for inclusion into the Air Force Lessons Learned Database **https://cs2.eis.af.mil/sites/12989/default.aspx**.

7.4.4. Evaluators submit lessons learned and after-action reports to MAJCOM OPSEC Program Managers within 45 days of completion of the exercise or operation when something significant or potentially useful was identified during the event. These documents are used to develop tactics improvement proposals IAW AFI 10-204, *Air Force Service Exercise Program and Support to Joint and National Exercise Program* and AFI 11-260, *Tactics Development Program*.

7.4.5. Lessons Learned Validation and Resolution: MAJCOM OPSEC Program Managers review and track lessons learned observations to ensure accuracy and applicability.

7.4.6. Concepts and ideas for exercise OPSEC scenarios are often identified from previous operational experiences, inspections, OPSEC program management assessments, OPSEC external assessments and ESSA support. Ideas and concepts to incorporate OPSEC into exercises are available from the AF OST.

Chapter 8

OPSEC REQUIREMENTS WITHIN ACQUISITIONS AND CONTRACTING

8.1. Incorporating OPSEC into the Acquisitions and Contracting Process. OPSEC must be considered throughout the lifecycle of the DoD Acquisitions and contractor-supported efforts. It is essential to integrate OPSEC into the earliest stages beginning with operational capabilities requirements generation and continue through the award process, design, development, test and evaluation, fielding, sustainment and system disposal. OPSEC requirements within acquisitions and contracting ensure critical information and/or indicators are not prematurely released to vendors. This applies to all types of contracts, including but not limited to service, support, acquisition and fundamental research and grants. Contractors for defense systems acquisition programs as well as other types of DoD contracts will practice OPSEC to protect critical information and indicators as specified in government contracts and subcontracts.

8.2. Organizational Responsibilities. Organizations requesting contract support determine and communicate the OPSEC measures required for each contract and ensure they are included in requests for proposal, statements of work, performance work statements, statement of operations, or other contract documents.

8.3. Document Reviews.

8.3.1. OPSEC Program Managers and OPSEC Signature Managers in coordination with the contract requirement owners are responsible for the review of contract documents to ensure critical information and/or indicators are not made available to the public. An approved Critical Information and Indicator List will be used as a reference when conducting reviews.

8.3.2. When an OPSEC Coordinator or Contracting representative is conducting the review, the OPSEC Program Manager/OPSEC Signature Manager provides technical guidance and an approved Critical Information and Indicators List to assist in the analysis of information within the contract documents.

8.3.3. If it is determined that a contract document contains critical information and/or indicators associated with the performance of the contract, the requesting organization will develop an OPSEC Plan to protect the critical information and/or indicators associated with the contract from cradle to grave.

8.3.4. The requesting organization will specify OPSEC requirements for unclassified and classified contracts in requests for proposal, statements of work, performance work statements, statement of operations, or other contract documents. **(T-1).**

8.3.4.1. Provide sufficient detail to ensure complete contractor understanding of the requirements to protect the critical information and/or indicators (e.g., what do you want the contractor to do, how do you want the contractor to comply, when do you want the contractor to comply, who is going to provide OPSEC training).

8.3.4.2. Do not include critical information and indicators in unclassified contract documents. **(T-0).**

8.3.4.3. Ensure DD Form 254, *Department of Defense Contract Security Classification Specification* is appropriately annotated IAW AFI 16-1406, *Air Force Industrial Security Program*, for classified contracts that require OPSEC measures. **(T-0).**

8.3.5. If required, organizations will provide the contractor a copy of the OPSEC Plan associated with the contract. **(T-2).**

MARK D. KELLY, Lt Gen, USAF
Deputy Chief of Staff, Operations

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Federal Information Security Modernization Act, (44 U. S. C 3554), 18 December 2014

National Security Decision Directive 298, *National Operations Security Program*, 22 January 1988

DoDI O-3600.02, *Information Operations (IO) Security Classification Guide*, 28 November 2005

DoDM 5200.01, Vol 2, *DoD Information Security Program; Marking of Classified*

Information, 24 February 2012

DoDM 5200.01, Vol 3, *DoD Information Security Program: Protection of Classified Information*, 24 February 2012

DoDM 5200.01, Volume 4, *DoD Information Security Program: Controlled Unclassified Information (CUI)*, 24 February 2012

DoDD 5205.02E, *DoD Operations Security (OPSEC) Program*, 20 June 2012

DoDM 5205.02-M, *DoD Operations Security (OPSEC) Program Manual*, 3 November 2008

DoDI 8560.01, *Communications Security (COMSEC) Monitoring and Information Assurance (IA) Readiness Testing*, 9 October 2007

JP 1-02, *DoD Dictionary of Military and Associated Terms*, March 2018

JP 3-13.3, *Joint Doctrine for Operations Security*, 6 January 2016

AFPD 10-7, *Information Operations*, 4 August 2014

AFI 10-204, *Air Force Service Exercise Program and Support to Joint and National Exercise program*, 12 April 2019

AFI 10-404, *Base Support and Expeditionary (BAS&E) Site Planning*, 27 August 2015

AFI 11-260, *Tactics Development Program*, 15 September 2011

AFI 14-104, *Oversight of Intelligence Activities*, 5 November 2014

AFI 16-1404, *Air Force Information Security Program*, 29 May 2015

AFI 16-1406, *Air Force Industrial Security Program*, 25 August 2015

AFI 17-201, Command and Control (C2) for Cyberspace Operations, 5 March 2014

AFI 33-332, *Air Force Privacy and Civil Liberties Program*, 12 January 2015

AFI 33-360, *Publications and Forms Management*, 1 December 2015

AFI 63-101/20-101, *Integrated Life Cycle Management*, 9 May 2017

AFI 65-601, Vol 1, *Budget Guidance and Procedures*, 16 August 2012

AFI 71-101, Vol 2, *Protective Service Matters*, 23 January 2015

AFI 90-201, *The Air Force Inspection System*, 20 November 2018

AFMAN 33-363, *Management of Records*, 1 March 2008

Adopted Forms

AF Form 847, Recommendation for Change of Publication

DD Form 254, Department of Defense Contract Security Classification Specification

Abbreviations and Acronyms

ACC—Air Combat Command

AETC—Air Education and Training Command

AFFOR—Air Force Forces

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

AOC—Air and Space Operations Center

COMSEC—Communication Security

DoD—Department of Defense

DoDD—Department of Defense Directive

DOPC—Defense OPSEC Planners Course

DRU—Direct Reporting Unit

EPRM—Enterprise Protection Risk Management

ESSA—Electronic System Security Assessment

FOA—Field Operating Agency

IAW—In Accordance With

IG—Inspector General

JP—Joint Publication

MAJCOM—Major Command

MICT—Management Internal Control Toolset

OPSEC—Operations Security

OST—OPSEC Support Team

SIPRNet—Secret Internet Protocol Router Network

Terms

Activity—A function, mission, action, or collection of actions.

Adversary—An individual, group, organization or government that must be denied critical information and indicators. Synonymous with competitor/enemy.

Association—The characteristic of an indicator that makes it identifiable or causes it to stand out. Key signature properties are uniqueness and stability.

Conduit—A pathway over which data or information is collected, passed, analyzed and delivered to decision makers.

Continuum of Learning—Career-long process of individual development where challenging experiences are combined with education and training through a common taxonomy to produce Airmen who possess the tactical expertise, operational competence, and strategic vision to lead and execute the full spectrum of Air Force missions.

Contracting Office—For the purposes of this instruction the contracting office is the office designated to support the requiring activity for contracting actions and business advice.

Contrast—The characteristic of an indicator that refers to differences observed between an activity's standard profile and its most recent or current actions.

Counterintelligence—Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities.

Critical Information—Specific facts (or evidence) about friendly intentions, capabilities, and activities needed by adversaries to plan and act effectively against friendly mission accomplishments.

Critical Information and Indicators List—That part of an OPSEC program or plan that conveys the organization or mission specific critical information and indicators to personnel as a reference of what information that must be protected via secure means or indicators that must be hidden from adversary collection methods.

Cyberspace Defense Analysis—The resources, tools, and manpower required to conduct the monitoring, collection, and analysis of information content transmitted across DoD electronic communication systems.

Electronic Communication—Any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature, transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic, or photo-optical system that affects interstate or foreign commerce, but does not include the following: any wire or oral communication; any communication made through a tone-only paging device; any communication from a tracking device as defined by 18 USC § 3117; electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds; 18 USC § 2510(12).

Electronic System Security Assessment—The monitoring, collection and analysis of information content transmitted across DoD electronic communications systems. ESSA evaluate an organization's OPSEC posture and determine the amount and type of information available to adversary collection entities.

Enterprise Protection Risk Management—**A** web-based, cross-disciplinary decision support tool for security compliance and risk assessments; facilitates and standardizes risk assessment processes and promotes early implementation of cost-effective countermeasures.

Essential Secrecy—The condition achieved from the denial of critical information and indicators to adversaries through the combined efforts of traditional security programs and the operations security process.

Essential Secret—Specific aspects of planned friendly operations that, if compromised, would lead to adversary identification of exploitable conditions and potential failure to meet the commander's objectives and/or desired end state.

Exposure—The characteristic of an indicator that refers to when and for how long an indicator is observed.

External-facing—Available via the Internet to authorized users from any location. A DoD Internet service being external-facing has no bearing on whether it is public or private, i.e., both public and private DoD Internet services may be external-facing.

Focused Look Assessment—Specific to a single Air Force core function, organization, mission set, capability, or weapon system. A Focused Look Assessment can cover multiple organizations, installations, or locations.

Formal Training Unit—A unit with a primary mission to train crew personnel according to approved syllabi.

Human Intelligence—A category of intelligence derived from information collected and provided by human sources.

Imagery Intelligence—The technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials.

Indicator—In operations security usage, data derived from friendly detectable actions and open-source information that an adversary can interpret and piece together to reach conclusions or estimates of friendly intentions, capabilities, or activities.

Information Operations—The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. Joint Publication 1-02. (Actions taken to affect adversary information and information systems while defending one's own information and information systems.)

Inherently Governmental Functions—Duties of appointed Air Force employees (military members and civilian employees, including direct-hire foreign national employees, but not including contractors or indirect-hire foreign national employees) authorized to make decisions on behalf of the Air Force.

Internet of Things—The technologies and devices that sense information and communicate it to the Internet or other networks and, in some cases, act on that information.

Measurement and Signature Intelligence—Information produced by quantitative and qualitative analysis of physical attributes of targets and events to characterize, locate, and identify targets and events, and derived from specialized, technically derived measurements of physical phenomenon intrinsic to an object or event.

Measures of Effectiveness—An indicator used to measure a current system state, with change indicated by comparing multiple observations over time.

Measures of Performance—An indicator used to measure a friendly action that is tied to measuring task accomplishment.

Military Deception—Actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.

Node—An element of a conduit that represents a person, place, or physical thing through which information passes. Nodes may or may not inject bias during their handling and retransmission of data or information.

Observable—Activities apparent to observers and/or collectors that might be analyzed and used by the decision maker. The combination of an indicator and an opposing force conduit or open-source reporting.

Open-source Information—Information that any member of the public could lawfully obtain by request or observation as well as other unclassified information that has limited public distribution or access.

Open Skies Treaty—The Treaty on Open Skies establishes a regime of unarmed aerial observation flights over the territories of its signatories. The Treaty is designed to enhance mutual understanding and confidence by giving all participants, regardless of size, a direct role in gathering information through aerial imaging on military forces and activities of concern to them.

Operational Profile—The sum of all indicators associated with the aspects of a given activity from beginning to end.

Operationalizing OPSEC—The culmination of planning, execution and evaluation of DoD activities to protect against adversarial collection and exploitation of critical information and indicators ensuring essential secrecy

Operations Security—A capability that uses a process to preserve friendly essential secrecy by identifying, controlling and protecting critical information and indicators that would allow adversaries or potential adversaries to identify and exploit friendly vulnerabilities.

OPSEC Analyst—The primary adviser to the OPSEC Program Manager, OPSEC Signature Manager and OPSEC Planner to help develop, coordinate and manage OPSEC. This individual is usually a contractor. The OPSEC analyst reviews and analyzes data or information associated with the protection of critical information and indicators.

OPSEC Coordinator—An individual trained in OPSEC located at a subordinate level, who works in coordination with the OPSEC program manager or primary representative.

OPSEC Countermeasure—Planned action to affect collection, analysis, delivery, or interpretation of information. OPSEC countermeasures include all activities that affect content and flow of critical information and indicators from collection to the decision maker. Countermeasures are generally offensive in nature and may require additional approval authorities and review criteria associated with choice of means employed.

OPSEC Disclosure—The release of critical information or indicators which has been identified by the information owner (commander/director) and any higher headquarters that could potentially jeopardizes the unit's ability to achieve the objectives of its mission or to adequately protect its personnel and/or equipment.

OPSEC External Assessment—The application of the OPSEC methodology by a team of external subject matter experts to conduct a detailed analysis of all activities associated with a specific organization, operation, activity, exercise, or support function by employing the known collection capabilities of potential adversaries.

OPSEC Implementation Plan—Describes how an organization will implement and execute OPSEC in day-to-day activities (Phase 0 Operations).

OPSEC Indicator—Friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information.

OPSEC Internal Assessment—An evaluative process using internal organizational assets to assess an organization's operations, activities, exercises, or supporting functions to determine if sufficient countermeasures are in place to protect against the loss of critical information and indicators. An OPSEC Internal Assessment may include self-generated OPSEC reviews.

OPSEC Measure—Planned action to conceal critical information and indicators from disclosure, observation or detection.

OPSEC Plan—The outcome of the OPSEC process that completes APEX Tab C-3-C and

critical information and indicators.

OPSEC Planner—A functional expert trained and qualified to plan and execute OPSEC.

OPSEC Practitioners—Individuals charged with developing, implementing, planning and assessing OPSEC. Includes individuals such as OPSEC Program Managers, OPSEC Signature Manager, OPSEC Coordinators, OPSEC Support Teams, OPSEC Instructors and OPSEC Planners.

OPSEC Program Management Assessment—**A**n in-depth evaluation of the implementation and effectiveness of an organization's OPSEC program. OPSEC program management assessments are conducted by a team of subject matter experts to provide a detailed analysis of an OPSEC program's effectiveness by completing a thorough analysis of how the program is implemented, executed, supported and managed.

OPSEC Program Manager—A full-time appointee or primary representative assigned to develop and manage an OPSEC program.

OPSEC Review—Methods to determine an organizations compliance with established OPSEC standards or measures of performance. Inspector General Inspections, or higher headquarters reviews that specifically address OPSEC are considered OPSEC Reviews.

OPSEC Signature Manager—An individual responsible for the active defense or exploitation of operational profiles resident at a given military unit.

OPSEC Support Capability—The range of capabilities used by the components to provide the required organize, train and equip to sustain their OPSEC efforts.

OPSEC Vulnerability—A condition in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated by an adversary in time to prove a basis for effective adversary decision making.

OPSEC Working Group—Designated body representing a broad range of line and staff activities within an organization that provides advice and support to leadership and all elements of the organization. This can be an OPSEC, SM, threat, or public affairs working group that addresses OPSEC concerns).

Personally Identifiable Information Breach—An actual or possible loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.

Profile—The characteristic of an indicator that refers to the sum of unique signatures and associations generated by a functional activity.

Profiling Process—Defining the local operating environment and capture process points that present key signatures and profiles with critical information value. This process is the deliberate effort to identify functional areas processes and the observables they produce to contribute to the overall signature of day-to-day activities and operational trends.

Range Of Military Operations—The general categories of operations within which the military participates to fulfill the general strategic goals of the US government. These operations are broadly defined as War and Operations Other Than War. War involves combat operations and has as its general goal the ability to fight and win. Operations Other Than War may involve noncombat or combat operations; the general goals of these operations are, respectively, promote peace and deter war/resolve conflict.

Risk—A measure of the potential degree to which protected information is subject to loss through adversary exploitation.

Risk Analysis—A method by which individual vulnerabilities are compared to perceived or actual security threat scenarios to determine the likelihood of compromise of critical information.

Risk Assessment—A process of evaluating the risks to information based on susceptibility to intelligence collection and the anticipated severity of loss.

Self-Assessment Communicator—A two-way communication tool designed to improve compliance with published guidance and communicate risk and program health up and down the chain of command in near real-time.

Sensor—The collection element of the conduit or information pathway which identifies, registers and subsequently transmits data.

Signals Intelligence—A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted.

Signature—Observable activities and operational trends that reveal critical information to adversary intelligence collection.

Signature Management—A systematic approach to identify, prioritize, and manage physical, technical, and administrative indicators of friendly forces' operational profiles that, if ignored, will be exploited by an adversary to achieve an operational advantage over friendly force objectives.

Social Media—An online social platform or site used to share information, communicate, and build relationships with the public.

Threat—The capability of an adversary coupled with his intentions to undertake any actions detrimental to the success of program activities or operations.

Threat Assessment—An evaluation of the intelligence collection threat to a program activity, system, or operation.

Transcript—All or part of a verbatim reproduction of an assessed communication and may include certain identifying information. It may also contain transcriber's comments or remarks to clarify or enhance understanding of the information presented.

Unsecured—Communications that do not use authorized cryptographic products or protected distribution systems.

Vulnerability—An exploitable condition in which the adversary has sufficient knowledge, time and available resources to thwart friendly mission accomplishment or substantially increase operational risk.

Vulnerability Analysis—A process that examines a friendly operation or activity from the point of view of an adversary, seeking ways in which the adversary might determine critical information in time to disrupt or defeat the operation or activity.