Best Practices for Security Office Staffing in Federal Facilities:

An Interagency Security Committee Guide

1st Edition
August 2016

Interagency
Security
Committee

This page was left intentionally blank.

Message from the Program Director

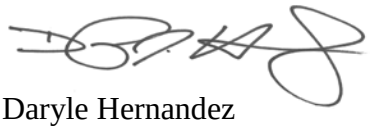
Protecting Federal employees and private citizens who work within and visit U.S. Government-owned or -leased facilities from all hazards is a complex and challenging responsibility. Comprising 58 Federal departments and agencies, the Interagency Security Committee's (ISC) primary mission is to develop security standards and best practices for non-military Federal facilities in the U.S.[1]

As Program Director of the ISC, I am pleased to introduce the *Best Practices for Security Office Staffing in Federal Facilities: An Interagency Security Committee Guide.* For the purposes of this document, the Security Office is defined as a centralized entity within an agency or an organization that has responsibility for security-related activities. Depending upon the structure and responsibilities assigned by the agency or organization, these security-related activities may include all or some combination of the following: physical security; personnel security; information security; access control; foreign ownership, control or influence (FOCI); communications security (COMSEC); Telecommunications Electronics Material Protected from Emanating Spurious Transmissions (TEMPEST); technical surveillance and countermeasures (TSCM); operations security (OPSEC); continuity of operations (COOP); occupant emergency plans (OEP); job classification; insider threat; workplace violence; and badging and personal identity verification (PIV) card issuance.

This document provides baseline recommendations to agencies by outlining basic security activities associated with implementing a Security Office staffing plan, incorporating lessons learned, and defining the key staffing requirements to achieve the mission of a Security Office. Furthermore, the document was developed to assist agencies in establishing criteria and policies which will ensure greater consistency in the application of staffing a Security Office for non-military, Federally-owned or -leased facilities.

Consistent with Executive Order (EO) 12977 (October 19, 1995), *Best Practices for Security Office Staffing in Federal Facilities: An Interagency Security Committee Guide* should be applied to all buildings and facilities in the U.S. occupied by Federal employees for non-military activities. These include existing owned; to be purchased or leased facilities; stand-alone facilities; Federal campuses; individual facilities on Federal campuses; and special-use facilities.

This guide is a significant milestone and represents exemplary collaboration across the ISC and among the ISC Security Office Staffing Working Group. With full concurrence, ISC primary members approved this guide on February 2016 and will review and update this guide as needed.



Daryle Hernandez
Program Director
Interagency Security Committee

[1] Additionally, in December 2012, the Department of Defense (DoD) adopted The Risk Management Process for Federal Facilities: an Interagency Security Committee Standard and integrated it into Unified Facilities Criteria (UFC) 4-010-01, DoD Minimum Antiterrorism Standard for Buildings, applicable to all off-installation leased spaced managed by DoD and all DoD-occupied space in buildings owned or operated by GSA.

Table of Contents

1 Introduction

The *Best Practices for Security Office Staffing in Federal Facilities* presents recommendations to the department/agency Director of Security or Chief Security Officer (CSO) for the development of a staffing plan. Effective workforce planning entails having the right number of people with the right skills working in the right jobs at the right time. In its simplest form, Security Office staffing refers to the examination of the total duties to be performed within the Security Office and the placement of properly trained and qualified personnel to perform those duties. Beyond that simple definition, the task of staffing can become a very complex issue.

Duties and responsibilities vary widely among Federal agencies and often within an agency's own divisions. Over time, personnel in security specialist positions gain knowledge and experience that may qualify them to perform numerous security tasks, while others may become more specialized, focusing on a single aspect of the security program. In some Security Offices, the security specialist may be required to perform several tasks to satisfy the requirements of the mission. As such, it is clear personnel planning plays an essential role in the proper staffing of a Security Office. Legacy security programs with existing robust security infrastructures may benefit from some of the information in this guide.

Security cognizance remains with each Federal department or agency unless lawfully delegated. For Title 50 agencies (i.e., agencies with an intelligence mission), the term Cognizant Security Agency is defined in EO 12829 as Executive Branch agencies that have been authorized by name to establish an Industrial Security Program to safeguard classified information under the jurisdiction of those agencies when disclosed or released to U.S. industry. The agencies currently designated are: the Department of Defense (DoD), the Department of Energy (DOE), the Nuclear Regulatory Commission (NRC), and the Office of the Director of National Intelligence (ODNI). The Secretary of Defense, the Secretary of Energy, the DNI, and the Chairman of NRC may delegate any aspect of security administration regarding classified activities and contracts under their purview, within the Cognizant Security Agency or to another Cognizant Security Agency. Responsibility for security administration may be further delegated by a Cognizant Security Agency to one or more cognizant Security Offices. It is the obligation of each Cognizant Security Agency to inform industry of the applicable cognizant Security Office.

This document is structured by topical area followed by a list of related questions to help determine the requirements for an organization's security office. It includes position classification for consideration based on the agency's needs and mission. Overall this document will assist a Federal department or agency in determining the personnel needs of its security office(s). Also provided in this document is a worksheet to aid in this process. Refer to Appendix A: Example of Security Activities Table. Relevant terms and expressions are defined in the Glossary of Terms.

2 Considerations for a Staffing Plan

Any Security Office should be organized and staffed to accomplish its mission of assuring full implementation of security policy goals. Methodology should be in place to identify required increases and decreases in staffing, and to identify technical, management, and/or support position skills needed to accomplish organizational functions based on planning goals and objectives. A myriad of requirements are also directed at the security function by various Federal agencies having special mandates for their area of interest. Position descriptions that identify staffing requirements and personnel management activities should be current and available. A formal security plan should be in place and updated annually, identifying training requirements and individual skills development for security staff employees as well as the expected security procedures and processes within the facility or element it governs. Security Office organization should be reviewed on a regular basis to evaluate functional alignments and appropriate staffing to accomplish the security mission. Clear and explicit delegations of authority and responsibility should be provided and documented at all levels.

2.1 Staffing Variables

Activities performed to satisfy the Security Office mission vary widely among Federal agencies and often within divisions of individual agencies. Variations are influenced by the following factors:

Mission	▪ What is the mission of the agency for which the Security Office is responsible?
Authority	▪ Is the authority granted to the Security Office limited or broad reaching? ▪ Is it the main office for the entire agency or for a satellite location? ▪ Does the Security Office have the final say or does final authority rest with higher level officials? ▪ What is the role or mix of roles of the Federal staff? Is the Federal staff in the oversight role of a contractor managed security program or will the Federal staff be responsible for filling the security roles?

Two key factors in determining staffing levels and security requirements are the agency and facility profile. The two profiles could influence the level of staffing for the Security Office at either the headquarters location or the field location based on various elements.

The following lists contains some considerations relative to the Facility Security Level (FSL) Determinations for Federal Facilities:[2]

[2] Please refer to the *Risk Management Process for Federal Facilities: An ISC Standard.*

Agency or Facility Population	▪ How many people work at the agency or facility on a day-to-day basis? o What are the hours they work? ▪ Do any require special security consideration (i.e., VIP status)? o How many people visit the agency or facility on a regular basis? o Are they members of the general public or other government employees? o Do they require security screening or special permission for entry?[3] ▪ What is the number and type of personnel on-site? o How many permanent vs. temporary staff? o How many Federal employees vs. contracted employees? o What are the type, volume, and frequency of routinely visiting staff vs. one-time visitors?
Agency or Facility Size	▪ Is the agency a cabinet-level or independent Federal agency? ▪ How large is the area for which the Security Office will be responsible? ▪ Is the entire operation contained within one facility or campus, or is it dispersed? If dispersed, how widely? ▪ How many buildings are involved? ▪ Will outlying areas require security protection?
Structure	▪ What type(s) of buildings (i.e., frame, brick, vault, etc.) or other structures require security protection? ▪ Is the exterior protected with fencing, barricades, guards, and guard stations? ▪ How many entrances/exits require protection? ▪ What types of physical security systems are in place (electronic and mechanical security systems include Physical Access Control Systems [PACS], Intrusion Detection Systems [IDS], Closed-Circuit Television [CCTV], metal detectors and x-ray scanning applications)?

[3] Not only is the employee population an important factor in developing a security staffing formula, but the degree to which the general public has access to the facility must be taken into account. The average population should be noted as well as considerations of special events or periods where the number of personnel fluctuates widely.

Location	▪ Is the agency or facility physically located on Federal property, in a shopping center, etc.? ▪ How close are the buildings to neighboring buildings/facilities and what types of activities are carried on in those neighboring buildings? ▪ Is the exterior protected with fencing, barricades, guards, and guard stations? ▪ Is the facility operating in a multi-tenant, owned or leased facility? ▪ Does the agency or facility operate at a controlled or uncontrolled location? ▪ Is the agency located near any commuter transit service(s) (e.g., airport, rail station, bus station)?
Information and Materials Handled	▪ Is classified information handled at the agency or facility? o If information at the site is classified, what classification level will require protection? The higher the level, the more control may be required. o If information at the site is classified, is there Restricted Data (RD) or Formerly Restricted Data (FRD)? Special requirements for access may apply. ▪ What categories or subcategories of Controlled Unclassified Information (CUI) are handled at the site (i.e., Privacy, Critical Infrastructure, Law Enforcement, etc.)? ▪ In what form is the classified and/or unclassified material at the site (i.e., equipment, chemicals, and documents)? ▪ Are there other types of controlled matter (e.g., accountable nuclear or radiological materials located on-site)? o Does the material(s) reside permanently on-site or is it leased (temporary)? ▪ Are there other types of assets at the site such as special nuclear material (SNM), sensitive compartmented information facilities (SCIF), special access program facilities, quantities of chemicals regulated by chemical facility anti-terrorism standards, biological agents, select agents and toxins, radiological sources, nuclear weapons, nuclear weapon components, or critical infrastructure?

2.2 Determination of Variables

To determine the variables for staffing, the CSO (or delegated security supervisor) should begin security program planning. This entails program management planning and a management budget process. These plans assist in the development of a security management organization and its staffing. The following must be considered:

Security Program Requirements	▪ What are the security policies from the national level through agency/department to office (i.e., EOs, Code of Federal Regulations [CFR], ISC Standards)? ▪ Who will be responsible for approving and documenting security plans, processes, and procedures?
Security Incident Management	▪ Is an Incident Command System (ICS) in place or does one have to be developed? ▪ Is there coordination with Federal response organizations and local response organizations? ▪ Is there a Memorandum of Agreement (MOA) for assistance in emergencies?
Corrective Actions	▪ What constitutes a need for corrective actions (i.e., security incidents, failure to meet specific requirements)? ▪ Who is responsible for documenting corrective action requirements? ▪ Who reviews corrective actions to ensure revisions effectively address failures or gaps?

3 Considerations of Security Areas and Topics

The below list was developed to provide baseline considerations for security concepts; however, it is by no means exhaustive. Some activities listed below will not apply to all facilities, while additional security considerations, not included herein, may be warranted based on the facility's specifications. The proper development of a staffing plan will require an analysis of all applicable activities for that facility. Within the security program requirements, the following areas and related staff should be considered.

3.1 Workplace Violence

The ISC published *Violence in the Federal Workplace: A Guide for Prevention and Response* (April 2013) to assist Federal departments and agencies in planning and mitigating acts of violence in the Federal workplace. The guide assists security planners for all buildings and facilities in the U.S. occupied by Federal employees for non-military activities. The guide also provides a variety of examples based on real-world events for planners to study and take into consideration.

DoD has published the *DoD Instruction 1438.06, January 16, 2014: DoD Workplace Violence Prevention and Response Policy*. The policy assigns responsibilities for workplace violence prevention and response policy regarding DoD civilian personnel in accordance with the authority in DoD Directive 5124.02. For additional information please refer to the cited documents.

3.2 Active Shooter

The ISC published the 2nd Edition *Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide* (non-FOUO) in November 2015. The FOUO version of this document was initially released to the Federal community only (July 2015). It streamlines existing ISC policy on active shooter incidents into one cohesive policy and guidance document to enhance preparedness for an active shooter incident at Federal facilities. The non-FOUO version was made publicly available as a reference document for the private sector so that a wider audience may benefit from the information presented therein. Due to the nature of an active shooter event, the document contains guidance for all who might be involved, including law enforcement agencies, facility tenants, and the public.[4]

3.3 Insider Threat

The ODNI defines the term insider threat as a person with authorized access to U.S. Government resources, to include personnel, facilities, information, equipment, networks, and systems, and uses the access to harm the security of the U.S. These threats encompass potential espionage,

[4] Users with a need-to-know may access the FOUO version of the standard (July 2015, 1st Edition). To request access, please send an e-mail to ISCAccess@hq.dhs.gov with your full name and contact information, including email, agency name, and reason for access.

violent acts against the Government or the Nation, and unauthorized disclosure of classified information, including the vast amounts of classified data available on interconnected U.S. Government computer networks and systems. The White House has established a *Presidential Memorandum, November 21, 2012* that speaks to the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs. The Memorandum provides direction and guidance to promote the development of effective insider threat programs within departments and agencies to deter, detect, and mitigate actions by employees who may represent a threat to national security.

DoD has also published the *DoD Directive 5205.16, September 30, 2014: The DoD Insider Threat Program*. The Directive establishes policy and assigns responsibilities within DoD to develop and maintain an insider threat program to comply with the requirements and minimum standards to prevent, deter, detect, and mitigate actions by malicious insiders who represent a threat to national security or DoD personnel, facilities, operations, and resources.

3.4 Physical Security

The ISC's *Risk Management Process for Federal Facilities* (August 2013) assists in determining both the level of physical security protection required and the risks associated with each office and the staffing requirements therein. Please refer to your agency's physical security policies as an additional reference.

3.4.1 Physical Security Elements

Implementation of architectural, procedural, and electronic/mechanical security system measures require not only the initial expenditure and oversight for their implementation, but a robust physical security program to ensure countermeasures remain effective.

Security Office Physical Security Functions	The size, quantity, mission, and population of an agency's facilities may impact the physical security staffing requirements of its Security Office. Consideration must be given to physical security activities provided internally and externally to the agency, including, but not limited to, the following: ▪ Protective Force ▪ Law Enforcement/Investigations ▪ Electronic and Mechanical Security Systems ▪ Identity Credentialing and Access Management (employees and visitors) ▪ Operations/Plans/Policy ▪ Security Project Management ▪ Accreditations (Classified National Security Information [CNSI] – Collateral Facilities and/or SCIFs) ▪ Physical Security Inspections and Assessments In the case of certain agencies, some of these functions may be significant enough that they serve as a separate entity within or outside the physical security function of the Security Office. Consideration should also be given to supplementation of personnel with technology. Capabilities may exist for processes that in the past were managed through human interaction; however, today can be accomplished through automation. Video monitoring with analytics, visitor pre-clearing/access enrollment software, and visitor kiosks are some examples of automation possibilities in physical security.
Protective Force	A protective force may be part of a security organization, or may be facility-specific. A proprietary protective force consisting of Federal law enforcement officers may be a part of a Security Office; or a contract security force may be specific to a facility or set of facilities, with Federal oversight falling under the Security Office. If the Security Office is responsible for establishing and scheduling training and standards or implementing and overseeing performance testing to ensure standards of protection, the staffing plan will reflect adequate personnel to support this effort.

Law Enforcement/ Investigations	Law enforcement and investigative functions may fall within the physical security element of a Security Office. This typically includes Federal officers responsible for response to an investigation of physical incidents within the confines of the agencies' owned or leased space. Consideration for staffing should account for quantity of facilities, level of protection (LOP) requirements of specific facilities, and agency mission needs. This support may be staffed internally or externally, depending on organizational structure and existing agreements.
Electronic and Mechanical Security Systems	Electronic and mechanical security systems include PACS, IDS, and CCTV; as well as, radios, security lighting, locks, keys, safes, and containers. Every Federal agency has some degree of requirements for these items, and ongoing maintenance support is necessary to ensure continuing functionality of systems. Depending on agency needs and budgets, maintenance support staffing for electronic and mechanical security systems is typically accomplished through a combination of Federal employees and contract security technicians.
Identity Credentialing and Access Management	Credentialing consists of identity verification and issuance of the Federal PIV credential and other credentials or badges used for physical and/or logical access, as applicable. Access management includes enrollment of PIV credentials or badges for facility access. This includes employee and visitor pre-screening (or verification of pre-screening) and access. Staffing typically includes a combination of Federal employee management and oversight, with contract support for processing visitors and issuing/enrolling employee PIV credentials and badges.
Operations/Plans/ Policy	Physical security elements within a Security Office require continually reviewed and updated written policies and procedures to maintain operations. Staffing of positions responsible for this function generally consists of seasoned and experienced senior physical security professionals.
Security Project Management	Growth, reduction, and changes in operation/mission within the Federal government result in continuous renovation and new construction projects for Federal facilities. Security requirements for these projects are driven by a wide variety of Federal standards, and oversight and management of security requirements is necessary from conception to completion. Staffing for smaller occasional build-outs may be accomplished as an additional duty if the subject matter expertise is available within a Security Office; however, for consistent and/or larger projects dedicated staff members, who are knowledgeable in construction methods and materials, security design, and Federal policy, are necessary.

Accreditations (CNSI – Collateral Facilities and/or SCIFs)	Accreditations of SCIFs and/or collateral spaces are a physical security function, but may fall within other elements of a Security Office or Federal agency, depending on the organization. Accreditation authority is typically held as an additional duty by senior personnel within the organization and may be delegated in some cases to dedicated full time staff to manage requirement development, administration, and inspections.
Physical Security Inspections and Assessments	Facility security assessments, compliance inspections, and other inspections/assessments are necessary to evaluate physical security program effectiveness and to continually improve and strengthen countermeasures. Agency-specific requirements, quantity of facilities, and external support are factors in determining staffing needs for inspections and assessments. Some agencies may be able to staff these functions as additional duties, where others may require dedicated full time employees.

3.5 Personnel Security

A Security Office should have a personnel security program policy to prevent unauthorized disclosure of sensitive and classified information to individuals who could cause irreparable damage to national security. The personnel security program manages and implements safeguards and security access authorization functions for each particular agency to specifically provide accurate, timely, and equitable determinations of individuals' eligibility for access to classified information, including SNM. The authorities for such, falls within the CFR 32 Part 147 and EO 12968; for DOE, the policy falls within 10 CFR 710 and DOE O 472.2. The personnel security program also addresses other functions, such as Government-wide requirements regarding access authorizations, i.e. security clearances, to include Administrative Review Procedures, the Homeland Security Presidential Directive-12 (HSPD-12/PIV), the FIPS 201-2, and the DOE O 206.2. HSPD-12 implements investigative and adjudicative policy for the Department's personal identity verification credentials. Personnel security program management and work practices support the accomplishment of U.S. Government missions in a secure environment by men and women in whom both the agencies and the American people may place their complete trust and confidence. Therefore, similar or like positions and jobs across Federal agencies should be classified or graded in a consistent manner because employees are evaluated against the same criteria rather than position-to-position comparisons.

Agencies are required to classify positions and job grade based on the duties and responsibilities assigned to the position and the qualifications required to perform that work. Qualifications possessed by an employee that are not needed to perform the work assigned to the position or job may not be considered in the position classification or job grading process. Some considerations include:

- Will personnel security activities be locally managed or centralized at a higher level?
- Are adjudications done on-site or at a different location?
- Is the site required to provide input such as disseminating and receiving documents for adjudications when they are done at a different location?

- Besides security investigations, what related activities are carried out by individuals at the site?
- What security clearance(s) is considered necessary for access to the site locations and information?
- What is required and who will provide other required security-related training? What method(s) will be used?
- Who will maintain training records (i.e., what was included in the training, who took it and when)?
- How will the processes used within the personnel section of the Security Office be determined, who will approve, and who will document and promulgate?

Additional references to personnel security policies that govern the personnel security process are included in the Reference Section of this document.

3.6 Information Security

The National Institute of Standards and Technology (NIST) defines Information Security (INFOSEC) as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.[5] In addition to NIST standards, in some cases, Classified National Security Systems (CNSS) policies will apply to classified information systems. (See NIST Special Publication 800-59 “Guideline for Identifying an Information System as a National Security System"). Please refer to your agency Chief Information Officer (CIO) for additional information.

Federal Information Processing Standards Publication 200 (FIPS Pub 200) addresses the minimum security requirements for Federal information and information systems. The minimum security requirements cover 22 security-related areas with regard to protecting the confidentiality, integrity, and availability of Federal information systems and the information processed, stored, and transmitted by those systems. The security-related areas to consider include:

- Who is responsible for access control?
- Who will conduct operations security training?
- Who has oversight for audit and accountability?
- Who is responsible for conducting certification, accreditation, and security assessments?
- Who has responsibility for configuration management?
- Who has authority for security input in contingency planning?
- Who is responsible for identification and authentication?
- Who provides incident response?
- Is maintenance a security responsibility?
- Who is responsible for media protection?
- Is security responsible for physical and environmental protection?
- Who conducts security planning?

[5]NIST IR 7298 Revision 2, Glossary of Key Information Security Terms

- Who performs personnel security functions?
- Who conducts risk assessment analysis?
- Is security responsible for security systems and services acquisition?
- Who develops system and communications protection plans?
- Does security perform system and information integrity?
- Does the agency have any automated systems that contain or process classified information?
- What signage is required to identify the level of classification allowed on those systems?
- Where are those systems located?
- What are the required physical protection mechanisms?
- Who promulgates any special handling or marking requirements for these programs?

The 22 areas represent a broad-based and balanced information security program that addresses the management, operational, and technical aspects of protecting Federal information and information systems. Policies and procedures play an important role in the effective implementation of enterprise-wide information security programs within the Federal government and the success of the resulting security measures employed to protect Federal information and information systems. Thus, organizations must develop and promulgate formal, documented policies and procedures governing the minimum security requirements set forth in this standard and must ensure their effective implementation.

3.6.1 Classified Information Protection and Control (CIPC)

The protection and control of classified information covers the entire life cycle of classified information, from origination to destruction. The following activities make up a CIPC program and the staffing necessary to achieve these activities should be considered. In some cases, these activities are completed by the Security Office staff, and in other cases, they may be handled by someone outside the Security Office. Knowing who has the understanding and capability to do each of the following tasks is critical:

Marking classified matter (including working papers)	▪ Who is responsible for the accuracy of marking classified matter? ▪ What marking is required?
Dissemination and access	▪ Who is responsible for ensuring personnel are trained on the dissemination requirements of any classified or controlled unclassified information to another individual? ▪ Who is responsible for ensuring personnel are trained on the transmission methods for classified or controlled unclassified information?
Storage equipment & requirements	▪ Who is responsible for ensuring storage equipment meets national standards? ▪ Who is responsible for combination control? ▪ What documentation is necessary for the storage equipment use and maintenance?

Transmission equipment & requirements	▪ Who is responsible for ensuring transmission equipment meets national standards? ▪ What documentation is necessary for transmission equipment purchase, maintenance and use?
Receiving classified matter	▪ How is classified matter received? ▪ How is it documented? ▪ Are classified document receipts used? ▪ Is there a classified document control log? ▪ Who is responsible for developing emergency handling of classified matter? ▪ Who is notified when classified matter has been provided to emergency personnel? ▪ Has an emergency procedure that involves potential access to classified matter been developed and promulgated?
Reproduction equipment & requirements	▪ Who is responsible for ensuring reproduction equipment meets national standards and does not allow for unauthorized access? ▪ What documentation and/or signage is necessary? ▪ What is the required process for use of the equipment? ▪ Who will be responsible for developing documentation for the requirements and procedures for reproduction of classified information?
Destruction equipment & requirements	▪ What type(s) of destruction equipment is necessary for the type of classified or CUI at the site? ▪ Who is responsible for ensuring the destruction equipment meets national standards? ▪ What documentation is necessary and who will be responsible for developing the documentation for the requirements and procedures for using destruction equipment
Special access programs and intelligence information (see EO 13526)	▪ Does the agency have any special access programs and/or intelligence information for which the Security Office is responsible? ▪ As new requirements are finalized, who will promulgate the implementation for the agency/site/facility?
Restricted data (see 10 CFP Part 1045)	▪ Does the agency have any RD, FRD, Data or Transclassified Foreign Nuclear Information (TFNI) for which the Security Office is responsible? ▪ Who promulgates policies for implementing RD requirements? ▪ Does the agency track who has access to RD? ▪ Who is responsible for training persons who have access to RD on the authorities required to classify and declassify RD and handling procedures?

3.6.2 Classification/Declassification/Downgrading

EO 13526, *Classified National Security Information*, prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism. Below are questions to be considered when addressing staffing needs for classifying, declassifying, and downgrading Federal government information:

- Who is authorized to classify, declassify, or downgrade classified information either originally or derivatively)?
- How is required training accomplished (when, by whom, etc.)?
- What is the process for a classification review?
- What classification level(s) is the information at the site/facility?
- Where are classification and declassification guides located and maintained?

10 CFR Part 1045, *Nuclear Classification and Declassification*, prescribes Government-wide policies for classification of RD and FRD. Employees with classification authority must receive the required training prior to classifying matter containing RD. Also, it is imperative that employees understand documents containing RD/FRD are not automatically declassified and can only be declassified by the appropriate authority.

Below are questions to consider when addressing staffing needs for classifying and declassifying RD and FRD:

- Who is responsible for training RD classifiers?
- How are RD classifiers designated?
- Who ensures RD classifiers have appropriate guidance?
- Who is responsible for coordinating the declassification of documents containing RD, TFNI, or FRD with DOE or DOE/DoD respectively?

3.6.3 Controlled Unclassified Information

EO 13556, *Controlled Unclassified Information*, establishes an open and uniform program for managing information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information that is classified under EO 13556, or the Atomic Energy Act, as amended. Below are questions to be considered when addressing staffing needs for CUI Programs:

- What categories or subcategories of CUI are used by organizational personnel (see the CUI Registry at http://www.archives.gov/cui/)?
- Does the organization provide education and training on the proper handling and safeguarding of CUI?
  - Is training provided prior to access to CUI?
  - How is required basic training accomplished (when, by whom, etc.)?
  - How is required specified training accomplished (when, by whom, etc.)?
- Does the organization have policies that implement the CUI Program?
  - Is portion marking required?
  - Are coversheets required?
- How does the organization define and evaluate controlled environments (i.e., where CUI is stored and handled)?
- Has the organization designated a CUI Senior Agency Official?

- Has the organization designated a CUI Program Manager?
- Does the organization have a system in place for organizational personnel to report incidents involving CUI?
- How does the organization destroy CUI?
    - What standards, if any, are used to destroy CUI (e.g., NIS TSP 800-88, etc.)?
- Does the organization enter into any contracts, grants, or other agreements (agreements) that require non-executive branch entities to handle CUI?
- How is CUI transmitted or shared with authorized recipients (e.g., encrypted transmissions, in transit tracking for packages or mail containing CUI, etc.)?

Each agency should receive guidance and awareness training from their agency Senior Agency Official (SAO)/Program Manager (PM) prior to implementing the above CUI considerations.

3.7 Foreign Ownership, Control or Influence

Security Office staffing decisions include FOCI determinations when applicable. FOCI is defined as any instance when a U.S. company has a foreign interest direct or indirect, through the ownership of a U.S. company's securities. This could include contractual arrangements or other means, to direct or decide matters affecting the management or operations of that company. This may result in unauthorized access to classified information or may adversely affect the performance of classified contracts.[6] Whenever a company has been determined to be under FOCI, the primary consideration should be the safeguarding of classified information. The Cognizant Security Authority is responsible for taking whatever interim action necessary to safeguard classified information, in coordination with other affected agencies as appropriate. A company determined to be under FOCI is ineligible for a Facility Clearance (FCL) unless and until security measures have been put in place to negate or mitigate FOCI.

DOE, NRC, and the DNI have the responsibility to determine whether or not a company is under FOCI at their sites and facilities. DoD holds that responsibility for the rest of the Government.

Questions concerning FOCI to be considered when staffing a Security Office include:

- Are there any companies determined to be under FOCI at the site or facility in question?
- Do those companies under FOCI have an FCL?
- What protections are needed until such time as the FCL is established for those companies?

3.8 Operations Security

OPSEC is a systematic and proven process by which the U.S. Government and its supporting contractors can deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive Government activities.

The operations security process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate

[6] DoD 5200.22-M, National Industrial Security Program Operating Manual (NISPOM) 2-300a

countermeasures. The process begins with an examination of the totality of an activity to determine what exploitable but unclassified evidence of classified activity could be acquired in light of the known collection capabilities of potential adversaries. Such evidence usually derives from open source data. Certain indicators may be pieced together or interpreted to discern critical information. Indicators most often stem from the routine administrative, physical, or technical actions taken to prepare for or execute a plan or activity. Once identified, indicators are analyzed against the threat to determine the extent to which they may reveal critical information. Commanders and managers then use these threats and vulnerability analyses in risk assessments to assist in the selection and adoption of countermeasures.[7]

Questions to be considered when establishing an OPSEC program for staffing a Security Office:

- Is there a specified assignment of responsibility for local OPSEC direction and implementation?
- Are there specified requirements to plan for and implement OPSEC in anticipation of and, where appropriate, during department or agency activities?
- Is there direction to use OPSEC analytical techniques to assist in identifying vulnerabilities and to select appropriate OPSEC measures?
- What measures exist to ensure that all personnel, commensurate with their positions and security clearances, are aware of hostile intelligence threats and understand the OPSEC process?
- Are annual reviews and evaluations conducted to improve the local OPSEC program?
- Is there interagency support and cooperation with respect to the local OPSEC program?
- Are there routine checks to ensure that employees are compliant with OPSEC regulations?
- Are information system access areas properly identified?
- Who is responsible for identifying information system access areas?

3.9 Communications Security

COMSEC is a component of information assurance that deals with measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications.[8] Within COMSEC there are several disciplines including:

- Cryptographic Security;
- Emission Security;
- Physical Security;
- Traffic-flow Security;
- Transmission Security; and
- Electronic Key Management System (EKMS).

Without securing communications systems and traffic that flows on those systems, organizations will find information may be unintentionally released. Should organizations be providing

[7]National Security Decision Directive Number 298, "National Operations Security Program," January 22, 1988

[8]NIST IR 7298 Revision 2, Glossary of Key Information Security Terms

classified services, there are requirements that must be followed, such as EKMS developed by the National Security Agency (NSA), to supply electronic keys around the encryption of the COMSEC devices. Each agency operating in the classified space has processes that follow EKMS.

Personnel working in the COMSEC area of security utilize standards such as NSA/Central Security Service (CSS) Policy Manual 3-16, NAG-14C, NAG-18, NSTISSI 4000, and perform several tasks including:

- Protecting COMSEC material and limiting access to individuals with a valid need-to-know;
- Receiving, cataloging, and ensuring COMSEC material is safeguarded and accounted for;
- Maintaining COMSEC accounting and related records;
- Conducting inventories;
- Performing material destruction;
- Developing curriculum for material users; and
- Providing services as an NSA COMSEC Account Manager.

In accomplishing these tasks, personnel also deal with a variety of equipment and training methodologies. This equipment can include, where applicable:

- Command, Control, Communications, Computers, and Intelligence (C4I) Systems;
- Keying Material (KEYMAT);
- Documents;
- Fax;
- Telephony;
- Secure Terminal Equipment; and
- Global System for Mobile Communications Cell Phones.

3.10 TEMPEST and Technical Surveillance Countermeasures

EO 13231, Section 8, Sub Section C, paragraph iii (CNSS instructions and mandates); Committee on National Security Systems Policy (CNSSP) 300, Section 3, mandates all department heads fund and maintain a TEMPEST program. Considerations include:

- Who is responsible for ensuring the agency or section maintains a TEMPEST program?
- Who is responsible for ensuring the funding of the TEMPEST program?
- Who is the certified TEMPEST technical authority?

TSCM services should be provided by certified, qualified, and trained personnel to detect, neutralize, and/or exploit a wide variety of hostile penetration technologies, devices, and hazards used to obtain unauthorized access to classified and sensitive information of the surveyed areas. Considerations include:

- Who conducts TSCM services within the facility?
- Who is responsible for requesting TSCM services?

TSCM services for government sensitive facilities should only be performed by employees or contractors who have been trained through the Government's Interagency Training Center. They should provide a professional and technical evaluation of the department’s technical security

posture that normally will consist of a thorough visual, electronic, and physical examination in and about the designated area.

3.11 Personnel Development and Training

A formal security plan should be in place and updated annually identifying training requirements and the need for individual skills development for security staff employees. The plan should address such questions as:

- Is there an existing training program (i.e., instructors, training records, program reviews, certification, and approvals)? If not, does a training program need to be developed?
- What positions require specialized training tailored to meet the specific needs of the agency's security program and the specific roles of employees?
- Will the security personnel be limited to performance of one specialty; or do they perform other duties as required and is additional training required to perform those duties (i.e., VIP protection and video monitoring, mail room personnel and custodians, couriers and escorts, etc.)?
- Is there a provision for new employee orientation?
- Who will be responsible for training employees and contractors?
- Who will approve and/or provide that training?
- Is training internal or external? If internal, how will information be presented?
- What recertification requirements exist?
- Who will be responsible for ensuring the presentation of the material is provided to those who require it?
- What will the required training cost?
- Who will maintain training records?

3.12 Continuity of Operations Plans and Exercises

COOP is defined as an effort within individual organizations to ensure they can continue to perform their essential functions during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies.[9]

Questions to be considered when establishing COOP plans and exercises while staffing a Security Office:

- What is the experience level required of the COOP project manager and the COOP staff?
- What are the expectations of the organization's continuity coordinator?
- How complex is the existing COOP plan and its supporting devolution and reconstitution plans?
- What is the current budget for the COOP program?
- Where is the COOP program in reference to the continuity program management cycle?

[9] FCD 1 http://www.fema.gov/media-library-data/1386609058779-b084a7230663249ab1d6da4b6472e691/2012-Federal-Continuity-Directive1.pdf

- When was the COOP plan last tested and/or externally evaluated; what were the results and lessons learned?
- What are the minimum staffing level and minimum qualifications requirements based on the above considerations?
- Does the COOP plan identify primary and alternate personnel staffing?

3.13 Occupant Emergency Plans

Security and emergency preparedness require coordinated prevention, protection, response, and recovery activities spanning the preparedness spectrum. At the national level, preparedness is facilitated by Presidential Policy Directive 8. Additional information for plan requirements and development can be found in the guide, *Occupant Emergency Plans –Development, Implementation, and Maintenance*, available at http://www.gsa.gov/graphics/pbs/OEP_Guide.pdf; OEP Supplement 1: Emergency Situations, available at http://www.gsa.gov/graphics/pbs/OEP_Guide_Supplement_1_situations.pdf; OEP Supplement 2 and 3: Template Instructions and Template, available at http://www.gsa.gov/graphics/pbs/OEP_Guide_Supplement_2_instructions.pdf; and OEP *Occupant Emergency Programs: An Interagency Security Committee Guide* could also assist with identifying plan requirements and developing an OEP.

OEPs must include trained personnel to evaluate the plans through drills/exercises and provide recommendations from the evaluations. The importance of exercises during the plan development process is described in the above-mentioned guide. Some considerations for staffing using OEPs include:

- Will the OEP be the responsibility of the Security Office or others?
- What is the role of this Security Office during emergency situations?
- Is an ICS in place or does one have to be developed?
- Is surge staffing required for security incidents or emergencies?
- Will off-site officials respond during incidents (i.e., local law enforcement, emergency medical services, fire department, etc.)?
    - How will they be given access to classified, locked, or otherwise limited-access areas?
- Who will organize and implement emergency drills?

3.14 Facility Closure Requirements

Like other offices, Security Offices may be affected by facility closures, such as: inclement weather, adversarial threats, hours of operation, moving, hazardous conditions, etc. For these types of closures, additional attention should be given to practice drills or exercises to ensure protection of classified information and safety of personnel. Several factors to consider for staffing include:

- What are the agency guidelines, directions, and plans that must be reviewed and followed?
- Who develops a detailed action plan for meeting sequestration requirements and a recovery plan once lifted, if implemented?
- Who are the key personnel that are critical to the agency's mission within the Security Office?

- How is facility access control to be modified to alleviate concerns about who has access to the facility?
- What are the possible problem areas or negative responses from customers when dealing with a smaller workforce, delays, and disruptions?
- Is there, or does there need to be, a plan for a lack of guard force or services for facility protection during a facility closure?
- If the facility is closed for an extended period, what security systems need to be modified to address the circumstances?
- Does a plan for furlough, reduced overtime, and elimination of hiring or backfilling positions need to be developed?
- What are the risks of leaving the facility unattended for long periods of time?
- Who informs all parties of actions the Security Office plans to take?

4 Classification and Job Design

Once the above has been reviewed for applicability, a staffing plan can be developed to ensure the success of the program. This listing is not all-inclusive, nor will everything listed above be required at every Security Office. The identified topics are intended to provide support for staffing requirement determinations. The personnel required to accomplish these activities will vary from location to location based on size, number of employees and contractors, and other assets.

Documentation of the final policies, procedures, and staffing is critical to the effective operation of any Security Office or program. This documentation may be centralized by use of technical policy writers rather than within each discipline or subject area if resources are a consideration. Coordination by the writer with each subject matter expert is essential for a thorough understanding of the requirements, procedures, etc. to be documented.

4.1 Position Classification Standards

Position classification standards encourage uniformity and equity in the classification of positions by providing a common reference across organizations, locations, and agencies. Classification standards may cover one or many occupations, and usually include a description of the work performed, official titles, and criteria for determining grades. Some broad standards are issued as "functional guides" and provide criteria for determining the grade level of work in multiple occupations. Position classification standards and guidance covering most Federal positions are accessible on the internet at: http://www.opm.gov/fedclass/index.asp and http://www.opm.gov/fedclass/html/fwsdocs.asp for trades, craft, and labor positions. The ISC's *Security Specialist Competencies* guideline also provides functions and skills for the various disciplines.

Performance requirements in this guide were written broadly to incorporate all regulatory and certification criteria and to ensure applicability across all agencies. Agencies have the flexibility to include additional performance requirements under any performance element to increase the usefulness and job specificity needed for their executives.

The Office of Personnel Management (OPM) has two major responsibilities performed by two offices. Classification and assessment policy sets Government-wide policy for the General Schedule (GS) and the Federal Wage System (FWS) by ensuring position classification standards are used to classify GS positions and job grading standards are used to grade FWS jobs. Merit system audit and compliance decides classification and job grading appeals from current Federal employees. A decision from OPM is the final administrative decision on appeals.

4.1.1 Classification of Managerial & Non-Managerial Positions

Supervisors in managerial positions have the authority under the *GS Supervisory Guide* to direct work of an organizational unit and are held accountable for the success of a specific line or staff function. They are responsible for monitoring and evaluating the progress of the organization toward meeting goals, work plans, schedules, and commitment of resources. As described in 5 U.S. Code (U.S.C.) 5104, such positions may serve as head or assistant head of a major

organization within a bureau, or direct a specialized program of difficulty, responsibility, and national significance.

In today's complex multi-threat environment, the Federal sector security manager must continually assess their organization's ability to fulfill the commitments, goals, and objectives that constitute its mission, purpose, and LOP. A comprehensive evaluation of available resources and capabilities is essential in identifying the organizational staffing needed to support adequate personnel and asset protection.

A position that has been identified as "supervisory" is typically classified by applying the *GS Supervisory Guide*. This guide can be used to evaluate the grade level of GS supervisory positions, regardless of the occupation. OPM has organizational design and position classification professionals who can assist in reviewing existing resources and processes and creating a foundation for organizational staffing. OPM's organization design and position classification experts have an organization-wide perspective that will assist in meeting current challenges regardless of how large or small organizational staffing needs may be. They are able to tailor their services and deliverables to meet requirements and will provide additional information regarding any of their services upon request. This guide will assist in preliminary staff planning.

The position of supervisor is one that accomplishes work through the direction of other people. Those directed may be subordinate Federal civil service employees, whether full-time, part-time, intermittent, or temporary; assigned military employees; non-Federal workers; unpaid volunteers; student trainees; or others. Supervisors exercise delegated authorities. A first-level supervisor personally directs subordinates without the use of other, subordinate supervisors. A second-level supervisor directs work through one layer of subordinate supervisors. A "full assistant" shares fully with a higher level supervisor in all phases of work direction, contractor oversight, and delegated authority over the subordinate staff. Below are considerations for classification of managerial positions:

Factors to Consider in Classifying Supervisory Positions	▪ Program Scope and Effect ▪ Organizational Setting ▪ Supervisory and Managerial Authority Exercised ▪ Number of Personnel Supervised ▪ Personal Contacts ▪ Difficulty of Typical Work Directed ▪ Other Conditions
Determination of the Top Security Manager Position	▪ Does the position answer to a presidential appointee, a member of the Senior Executive Service (SES), a GS-15, a GS-14 or other GS level positions? ▪ Is the Security Office considered co-equal with other departments within the agency? If so, what is the level of their top executives? ▪ Are the duties of the lead position commensurate with the typical duties of an SES, GS-15, GS-14 or other GS level positions?

Senior Executive Service	The SES includes most managerial, supervisory, and policy positions classified above GS-15 or equivalent positions in the Executive Branch of the Federal Government. The SES is charged with leading the continuing transformation of government. These leaders possess well-honed executive skills and share a broad perspective of government and a public service commitment that is grounded in the Constitution. The keystone of the Civil Service Reform Act of 1978, the SES was designed to be a corps of executives selected for their leadership qualifications. Due to their backgrounds, SES team members are able to interpret evolving trends, legislation, and regulations. These experts can also anticipate new regulations and assist organizations in successfully navigating the ever-changing landscape in order to satisfy compliance, minimize negative impact, and maximize the ability to do business or otherwise function. In general, the SES member is responsible for developing and implementing security-related policies that guide Federal, state, or international government activities. They will provide direction, coordinate operations, and plan for future strategies. Primary responsibilities include: ▪ Managing and directing security work force. ▪ Ensuring maximum returns on investments. ▪ Increasing worker productivity. ▪ Negotiating contracts and agreements with Federal and state agencies and other organizations and preparing budgets for funding and implementation of programs. ▪ Evaluating research and studies to help formulate policies. ▪ Recommending improvements for programs and services. ▪ Directing, coordinating, and conducting activities between U.S. Government and foreign entities. ▪ Hiring, training, and testing personnel. ▪ Organizing, promoting, and coordinating support programs with non-Federal public service entities. ▪ Delivering speeches, composing articles, and presenting information for organization at meetings or conventions to promote services, exchange ideas, and accomplish objectives. ▪ Creating and maintaining records. ▪ Planning, directing, and coordinating operational activities at the highest level of management with the help of subordinate managers. ▪ Conducting and presiding over investigations to resolve complaints and violations. ▪ Submitting reports concerning government statutes.

The Personnel Classification of Non-Managerial Positions	The personnel classification of non-managerial positions will depend largely on those duties performed on a regular basis. The Security Activities Table (Appendix A) below lists activities normally conducted in a facility security setting. The table can be used for evaluating the current status of an existing Security Office; or can be used for planning a startup staffing operation. Some of the duties may currently be performed primarily by managerial positions. The precise delineation of duties may depend on other circumstances such as number of staff, the abilities of the personnel, etc.

4.2 Assessment of Current Staffing

To begin, the office will need to assess the current management of the organization's positions and develop a framework for an effective staffing program. In a staffing analysis, it is necessary to review the types, grades, and numbers of positions in comparison with functions and workload; review position descriptions for accuracy and clarity; compute supervisory ratios; and assess career paths, career ladders, and the balance between support positions and those assigned to perform the mission-oriented functions of the organization. After this process, a written analysis of the findings should be delivered along with recommendations for achieving greater efficiency and cost-effectiveness. In meeting this objective, the Security Office should consider:

- Comprehensive organizational reviews;
- Occupational analyses;
- Workforce composition and skills utilization assessments;
- Alignment or assessment of organization structures and human capital;
- Distribution of work assignments;
- Position formulations and descriptions;
- Implementation of organizational decisions;
- Position management analysis;
- Strategies to determine future human capital needs;
- On-site or virtual desk audits;
- Development of position descriptions;
- Review of standardized position descriptions;
- Development or review of position description libraries;
- Development of comprehensive or standard evaluation statements; and
- Participation in customized workshops on classification principles and policies.

Additional references for current, contingent, and optimal security processes and procedures conducted by current personnel or anticipated personnel are included in Appendix A of this document.

4.3 Security Office Span of Control

Security Offices are dynamic entities that grow and change within the risk environment in which they operate. A considerable amount of effort can be expended in redesigning roles and responsibilities for security managers and determining the best organizational structure for

protecting personnel and property against existing threats within budget constraints. A key element of organizational design strategy that can be particularly challenging to determine is span of control. The following are some of the considerations governing span of control:

Geographical Dispersion	If the branches of an agency are widely dispersed, then the manager may find it difficult to supervise each of them; as such the span of control will be smaller.
Competence of Workers	If workers are highly competent, they may need little supervision and can be left on their own; as such, the span of control will be wider.
Qualifications of Supervisor	An experienced supervisor with a good understanding of the tasks, good knowledge of the subordinates, and good relationships with the subordinates will be able to supervise more workers.
Developmental Actions of Supervisor	A supervisor that enhances performance of the subordinates by training and developing new skills in the workers will need less span of control than one who is focused only on performance management.
Similarity of Tasks	If the tasks that the subordinates are performing are similar, then the span of control can be wider, as the manager can supervise them all at the same time.
Volume of Other Tasks	If the supervisor has other responsibilities, such as membership of committees, involvement in other projects, or liaising with stakeholders, the number of direct reports will need to be smaller.
Required Administrative Tasks	If the supervisor is required to have regular face-to-face meetings, complete appraisal and development plans, discuss remuneration benefits, write job descriptions and employment contracts, explain employment policy changes, and perform other administrative tasks, then the span of control is reduced.

5 References

- National Security Decision Directive Number 298, “National Operations Security Program,” January 22, 1988
- NIST IR 7298 Revision 2, Glossary of Key Information Security Terms, May 31, 2013
- DoD 5200.22-M, National Industrial Security Program Operating Manual (NISPOM) 2-300a
- FCD 1 http://www.fema.gov/media-library-data/1386609058779-b084a7230663249ab1d6da4b6472e691/2012-Federal-Continuity-Directive1.pdf
- Atomic Energy Act of 1954, as amended
- EO 13526, “Classified National Security Information,” December 29, 2009
- 32 CFR 2001, “Classified National Security Information: Final Rule,” June 25, 2010
- 10 CFR 1045, “Nuclear Classification and Declassification,” December 31, 1997
- Multi-Year Strategy and Program Management Plan (MYSPMP) Template at https://www.fema.gov/media-library/assets/documents/92169
- Violence in the Federal Workplace: A Guide for Prevention and Response, 1st Edition April 2013
- DoDI 1438.06, January 16, 2014: DoD Workplace Violence Prevention and Response Policy
- DoD Directive 5205.16, September 30, 2014: The DoD Insider Threat Program
- Presidential Memorandum - National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs
- Title 5, U.S. Code, Section 552(a), "Records maintained on individuals" [The Privacy Act of 1974, as amended]
- Title 5, U.S. Code (U.S.C.), Section 7532, "Suspension and removal"
- EO 10450, as amended, "Security Requirements for Government Employment," April 27, 1953
- EO 12958, as amended, "Classified National Security Information," April 17, 1995
- EO 12968, as amended, "Access to Classified Information," August 2, 1995
- EO 13467, as amended, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information," June 30, 2008
- EO 13488, "Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust," January 16, 2009
- EO 13556, “Controlled Unclassified Information,” November 4, 2010.

6 Interagency Security Committee Participants

ISC Chair
Caitlin Durkovich
Assistant Secretary for Infrastructure Protection
U.S. Department of Homeland Security

Program Director
Daryle Hernandez
Interagency Security Committee

ISC Operations Director
Bernard Holt
Interagency Security Committee

ISC Working Group Chair
Linda Ruhnow
Department of Energy

Working Group Members

William Morrison
Federal Aviation Administration

Dwayne Deaver
Department of Justice

Tarkeisha Wills
Office of Personnel Management

John Tigmo
Department of Commerce

Thomas McGoff
Federal Protective Service

Dairel Rawson
Office of Personnel Management

Charles King
Federal Trade Commission

Antonio Reynolds, Sr.
Interagency Security Committee

Salvatore Ingraldi
Department of Defense

Megan K. Drohan
Interagency Security Committee

Donald Cooper
Federal Protective Service

Jesse Williamson
Interagency Security Committee

Appendix A: Example of Security Activities Table

The following example serves as a consolidated list of considerations for current, contingent, and optimal security processes and procedures conducted by current personnel or anticipated personnel. By completing this table, the department/agency Director of Security, CSO, or their designee should be able to determine whether the staffing of the Security Office being analyzed is sufficient and appropriately allocated or if additional personnel are required. It can be used to reorganize a Security Office based on the priorities of that office or develop a plan for a new Security Office. By estimating the number of hours spent in a month on the activities for which they are responsible and noting how many full-time equivalent (FTE) employees are currently fulfilling those duties (whether Federal or contractor, at what grade or salary level, and their titles), it should become obvious as to whether or not additional staffing would be required to fulfill those duties under both acceptable and ideal circumstances. It would also allow for an estimate of what the staffing requirements would be for that activity to be performed at optimum capacity. It may be that the current staffing is sufficient, or it may indicate that additional personnel should be added. Noting the priority of the activities within the office or facility will provide the ability to determine where assets should be applied to obtain the maximum benefit with the assets available and in what order new assets should be applied to these activity areas. It can also provide insight into where personnel should be provided additional training in order to assist in different activities and/or to assist in other high priority areas when necessary. It can also be used to provide support for requests for additional personnel.

ACTIVITIES	**Approximate Number of Hours per Month**	**Current Staffing(# FTEs)**	**Federal Employee or Contractor**	**Federal Employee Grade Level**	**Position Title**	**Optimal Staffing (# FTEs)**	**Priority Within Topical Area**
Physical Security (3.3)							
Access Control							
Alarms							
Badging							
Barrier Installation and Maintenance							
Develop and Document Local Procedures							
Development of Security Areas							
Executive Protection							
Protective Security Officer Force							
Facility Security Assessments							
Intrusion Detection Systems: Research, Purchase, Installation, and Maintenance							

ACTIVITIES	Approximate Number of Hours per Month	Current Staffing(# FTEs)	Federal Employee or Contractor	Federal Employee Grade Level	Position Title	Optimal Staffing (# FTEs)	Priority Within Topical Area
Locks and Key Maintenance							
Performance Tests							
Training							
Weapons Procurement and Maintenance							
Radio Systems							
Security Lighting							
Personnel Security (3.4)							
Adjudication							
Document Local Procedures							
New Employee Orientation							
Reciprocity							
Security Investigations							
Training							
Information Security (3.5)							
Classification/Declassification/ Downgrading							
Classified Matter Protection and Control							
Controlled Unclassified Information							
Destruction equipment and requirements							
Marking							
Receiving Classified Matter							
Reproduction Equipment and Requirements							
Special Access Programs and Intel Information							
Storage Equipment and Requirements							
Systems Security							

ACTIVITIES	Approximate Number of Hours per Month	Current Staffing(# FTEs)	Federal Employee or Contractor	Federal Employee Grade Level	Position Title	Optimal Staffing (# FTEs)	Priority Within Topical Area
Transmission Equipment and Requirements							
Industrial Security (3.6)							
FOCI and Facility Clearance							
Operations Security (3.7)							
Analyze Threats, Vulnerabilities, and Risks							
Annual Review							
Awareness							
Compliance Measures							
Determine and Apply Countermeasures							
Identify Critical Information							
Communications Security (3.8)							
Cryptographic Security							
Electronic Key Management System							
Emission Security							
Physical Security							
Traffic-flow Security							
Transmission Security							
TEMPEST and Technical Surveillance Countermeasures (3.9)							
Maintenance, Funding, Certification							
Personnel Development & Training (3.10)							

ACTIVITIES	Approximate Number of Hours per Month	Current Staffing(# FTEs)	Federal Employee or Contractor	Federal Employee Grade Level	Position Title	Optimal Staffing (# FTEs)	Priority Within Topical Area
Annual Training							
New Employee Orientation							
Specialized Training Programs							
Continuity of Operations and Exercises (3.11)							
COOP Exercises							
Develop and Document Basic COOP Plan							
Occupant Emergency Plans (3.12)							
Contingency Staffing Plans/Locations							
Develop and Document Procedures							
Incident Command System							
Test and Evaluate Plan							
Facility Closure Requirements (3.13)							
Coordination of Plans with other Federal Agencies							
Staffing Requirements Plans for Closures							

List of Abbreviations/Acronyms/Initializations

TERM	DEFINITION
C4I	Command, Control, Communications, Computers, and Intelligence
CCTV	Closed-Circuit Television
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CIPC	Classified Information Protection and Control
CNSI	Classified National Security Information
CNSS	Classified National Security Systems
CNSSP	Committee on National Security Systems Policy
COMSEC	Communications Security
COOP	Continuity of Operations
CSO	Chief Security Officer
CSS	Central Security Service
CUI	Controlled Unclassified Information
DNI	Director of National Intelligence
DoD	Department of Defense
DOE	Department of Energy
EKMS	Electronic Key Management System
EO	Executive Order
FCL	Facility Clearance
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
FOCI	Foreign Ownership, Control or Influence
FOUO	For Official Use Only
FRD	Formerly Restricted Data
FSL	Facility Security Level

TERM	DEFINITION
FTE	Full Time Equivalent
FWS	Federal Wage System
GS	General Schedule
HSPD	Homeland Security Presidential Directive
ICS	Incident Command System
IDS	Intrusion Detection System
INFOSEC	Information Security
ISC	Interagency Security Committee
KEYMAT	Keying Material
LOP	Level of Protection
MEF	Mission Essential Functions
MOA	Memorandum of Agreement
MYSPMP	Multi-Year Strategy and Program Management Plan
NEF	National Essential Functions
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OEP	Occupant Emergency Plan
OPM	Office of Personnel Management
OPSEC	Operations Security
OUO	Official Use Only
PACS	Physical Access Control Systems
PIV	Personal Identity Verification
PM	Program Manager
PMEF	Primary Mission Essential Functions

TERM	DEFINITION
RD	Restricted Data
SAO	Senior Agency Official
SCIF	Sensitive Compartmented Information Facility
SES	Senior Executive Service
SNM	Special Nuclear Material
TEMPEST	Telecommunications Electronics Material Protected from Emanating Spurious Transmissions
TFNI	Transclassified Foreign Nuclear Information
TSCM	Technical Surveillance Countermeasures
UCNI	Unclassified Controlled Nuclear Information
U.S.C.	United States Code

Glossary of Terms

TERM	DEFINITION
Cognizant Security Agency	DoD, DOE, NRC, and ODNI. The Secretary of Defense, the Secretary of Energy, the DNI, and the Chairman of NRC, may delegate any aspect of security administration regarding classified activities and contracts under their purview within the Cognizant Security Agency or to another Cognizant Security Agency.[10]
Cognizant Security Authority	The single principal designated by a Senior Official of the Intelligence Community to serve as the responsible official for all aspects of security program management concerning the protection of national intelligence, sources and methods, under SOIC responsibility.[11]
Communications Security	A component of Information Assurance that deals with measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes crypto security, transmission security, emissions security, and physical security of COMSEC material.[12]
Continuity of Operations	An effort within individual organizations to ensure they can continue to perform their essential functions during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies.[13]
Continuity Plan	A plan that details how an individual organization will ensure it can continue to perform its essential functions during a wide range of emergencies.[14]
Continuity Program Management Cycle	An ongoing, cyclical model of planning, training, evaluating, and implementing corrective actions for continuity capabilities.[15]
Controlled environment	Any area or space an authorized holder deems to have adequate physical or procedural controls (e.g., barriers or managed access controls) to protect CUI from unauthorized access or disclosure.

[10] National Industrial Security Program Operating Manual, DoD 5220.22-M, February 28, 2006

[11] Office of the Director of National Intelligence, Intelligence Community Standard Number 2008-700-1

[12] NIST IR 7298 Revision 2, Glossary of Key Information Security Terms

[13] FCD 1 http://www.fema.gov/media-library-data/1386609058779-b084a7230663249ab1d6da4b6472e691/2012-Federal-Continuity-Directive1.pdf

[14] FCD 1 http://www.fema.gov/media-library-data/1386609058779-b084a7230663249ab1d6da4b6472e691/2012-Federal-Continuity-Directive1.pdf

[15] FCD 1 http://www.fema.gov/media-library-data/1386609058779-b084a7230663249ab1d6da4b6472e691/2012-Federal-Continuity-Directive1.pdf

TERM	DEFINITION
Controlled Unclassified Information (CUI)	Information the Government creates or possesses that a law, regulation, or Government-wide policy requires or permits an agency to handle by means of safeguarding or dissemination controls.
CUI Registry	The online repository for all information, guidance, policy, and requirements on handling CUI. http://www.archives.gov/cui/
Facility	Space built or established to serve a particular purpose. The facility is inclusive of a building or suite and associated support infrastructure (e.g., parking or utilities) and land.[16]
Facility Clearance	An administrative determination that, from a national security standpoint, a facility is eligible for access to classified information at the same or lower classification category as the clearance being granted.[17]
Foreign Ownership, Control or Influence	Designation for a U.S. company when a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable through the ownership of the U.S. company's securities, by contractual arrangements or other means, to direct or decide matters affecting the management or operations of that company in a manner which may result in unauthorized access to classified information or may adversely affect the performance of classified contracts.[18]
Federal Wage System	A uniform pay-setting system that covers Federal appropriated fund and non-appropriated fund blue-collar employees who are paid by the hour. The FWS ensures Federal trade, craft, and laboring employees within a local wage area who perform the same duties receive the same rate of pay.[19]
Incident Command System	A management system designed to enable effective and efficient domestic incident management by integrating a combination of facilities, equipment, personnel, procedures and communications operating within a common organizational structure.[20]
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.[21]

[16] August 2013/1st Edition Risk Management Process: An Interagency Security Committee Standard

[17] http://www.dss.mil/isp/fac_clear/per_sec_clear_proc_faqs.html

[18] DoD 5200.22-M, National Industrial Security Program Operating Manual (NISPOM) 2-300a

[19] http://www.opm.gov/policy-data-oversight/pay-leave/pay-systems/federal-wage-system/

[20] http://www.fema.gov/national-incident-management-system/incident-command-system-resources

[21] NIST IR 7298 Revision 2, Glossary of Key Information Security Terms

TERM	DEFINITION
Information Security Program Plan	A formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.[22]
Intrusion Detection System	Hardware or software product that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations).[23]
Keying Material	Key, code, or authentication information in physical, electronic, or magnetic form.[24]
Level of Protection	The degree of security provided by a particular countermeasure or set of countermeasures. Levels of protection used in this Standard are Minimum, Low, Medium, High, and Very High.[25]
Memorandum of Agreement	Written agreements between organizations that require specific goods or services to be furnished or tasks to be accomplished by one organization in support of the other.[26]
National Essential Functions (NEF)	The eight functions that are necessary to lead and sustain the Nation during a catastrophic emergency and that, therefore, must be supported through COOP and continuity of government capabilities.[27]
Occupant	Any person who is permanently or regularly assigned to the government facility and displays the required identification badge or pass for access, with the exception of those individuals providing a service at the facility (guards, custodians, etc.). The Facility Security Committee establishes the thresholds for determining who qualifies for "occupant" status.[28]

[22] NIST IR 7298 Revision 2, Glossary of Key Information Security Terms

[23] NIST IR 7298 Revision 2, Glossary of Key Information Security Terms

[24] NIST IR 7298 Revision 2, Glossary of Key Information Security Terms

[25] August 2013/1st Edition Risk Management Process: An Interagency Security Committee Standard

[26] FCD 1 http://www.fema.gov/media-library-data/1386609058779-b084a7230663249ab1d6da4b6472e691/2012-Federal-Continuity-Directive1.pdf

[27] FCD 1 http://www.fema.gov/media-library-data/1386609058779-b084a7230663249ab1d6da4b6472e691/2012-Federal-Continuity-Directive1.pdf

[28] August 2013/1st Edition Risk Management Process: An Interagency Security Committee Standard

TERM	DEFINITION
Occupant Emergency Plan	A short-term emergency response plan, which establishes procedures for evacuating buildings or sheltering-in-place to safeguard life and property.[29]
Operations Security	Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities.[30]
Primary Mission Essential Functions	Those organization Mission Essential Functions (MEFs), validated by the National Continuity Coordinator, which must be performed in order to support the performance of NEFs before, during, and in the aftermath of an emergency. PMEFs need to be continuous or resumed within 12 hours after an event and maintained for up to 30 days or until normal operations can be resumed.[31]
Security Program Plan	Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management security controls and common security controls in place or planned for meeting those requirements.[32]
Technical Surveillance Countermeasure	Techniques and measures to detect and nullify a wide variety of technologies that are used to obtain unauthorized access to classified national security information, restricted data, formerly restricted data and/controlled unclassified information.[33]

[29] FCD 1 http://www.fema.gov/media-library-data/1386609058779-b084a7230663249ab1d6da4b6472e691/2012-Federal-Continuity-Directive1.pdf

[30] NIST IR 7298 Revision 2, Glossary of Key Information Security Terms

[31] FCD 1 http://www.fema.gov/media-library-data/1386609058779-b084a7230663249ab1d6da4b6472e691/2012-Federal-Continuity-Directive1.pdf

[32] NIST IR 7298 Revision 2, Glossary of Key Information Security Terms

[33] 32 CFR Part 149 – Policy on Technical Surveillance Countermeasures