NOT MEASUREMENT SENSITIVE

DOE-HDBK-1233-2019
June 2019

DOE HANDBOOK

OPERATIONS SECURITY (OPSEC)

U.S. Department of Energy **AREA SANS**
Washington, DC 20585

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

This page intentionally left blank.

FOREWORD

The protection of classified information, projects, and missions is of paramount importance in fulfilling security responsibilities in connection with the Department of Energy (DOE). Operations Security (OPSEC) involves a process of determining unclassified or controlled critical information that may be an indicator or pathway to classified or sensitive activities requiring protection, whether for a limited or prolonged time. To ensure protection, employees should know and follow the applicable procedures and processes outlined in national and departmental policies.

This handbook does not establish new requirements and any existing requirements are explicitly referenced from national policy or a DOE Order using the terms "must" or "shall." It is not intended to replace DOE Order 471.6, *Information Security,* other departmental rules, or national directives. This handbook describes one way to fulfill requirements for OPSEC within DOE.

- Section 1 identifies the purpose, history and basic understanding of OPSEC.
- Section 2 describes the general OPSEC Program and the specific OPSEC Program Plan and its components.
- Section 3 discusses the OPSEC five-step process. It provides methods to identify critical information, the potential threat, vulnerabilities, and types of countermeasures that may be used.
- Section 4 describes the on-going activities that keep the critical information and related information and threats up to date. Trainings, briefing and awareness activities are provided.
- Appendix A is a copy of National Security Decision Directive 298, *National Operations Security Program.*
- Appendix B contains a sample OPSEC plan.
- Appendix C provides a sample OPSEC assessment report.
- Appendix D provides a sample threat statement.
- Appendix E contains a sample website review template.
- Appendix F provides the IOSS OPSEC program implementation tiers.

In addition to the sample plans, reports and posters described above, additional resources and information may be found under Security Policy Guidance Documents on DOE Powerpedia at https://powerpedia.energy.gov/wiki/Office_of_Security_Policy. Samples may also be submitted for consideration and inclusion, as appropriate.

Beneficial comments (recommendations, additions, and deletions), as well as any pertinent data that may be of use in improving this document, should be emailed to Security.Directives@hq.doe.gov or addressed to:

Office of Security Policy (AU-51)
Office of Environment, Health, Safety and Security (AU)
U.S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585

TABLE OF CONTENTS

FOREWORD i
ACRONYMS vi
1.0 INTRODUCTION 7
1.1 Purpose 7
1.2 Understanding OPSEC 8
1.2.1 History 8
1.2.2 Current Application 8
2.0 ESTABLISH AN OPSEC PROGRAM 9
2.1 OPSEC Program Plan 9
2.2 Identification of Roles and Responsibilities 10
2.2.1 Site – Federal, Contractor, and Tenant Organizations 10
2.3 Establish an OPSEC Working Group 11
2.4 Coordination and Communication 12
2.4.1 Office of Intelligence/Counterintelligence 12
2.4.2 Internal and External Organizations 12
2.4.3 Foreign Visits and Assignments 13
3.0 APPLY THE OPSEC FIVE-STEP PROCESS 14
3.1 Step 1 – Identification of Critical Information 15
3.1.1 Development and Prioritization of Critical Information List 15
3.1.2 Elements of Critical Information 16
3.1.3 Indicators and Pathways 16
3.1.4 OPSEC Reviews 18
3.1.5 Public Release Review 18
3.2 Step 2 – Analysis of Threats 21
3.2.1 Intelligence Cycle 22
3.2.2 National Threats 24
3.2.3 Site-Specific Threats 26
3.2.4 Collection Techniques 27
3.3 Step 3 – Analysis of Vulnerabilities 32
3.3.1 OPSEC Assessments 33
3.3.2 Phase 1 – Planning and Preparation 36
3.3.3 Phase 2 – Team Orientation 37
3.3.4 Phase 3 – Introductory Briefing 37
3.3.5 Phase 4 – Field Data Collection 37
3.3.6 Phase 5 – Data Analysis 47

3.3.7 Phase 6 – Draft Report 47
3.3.8 Phase 7 – Exit Briefing........ 48
3.3.9 Phase 8 – Final Report 48
3.3.10 Phase 9 – Follow-on Tasks........ 48
3.3.11 Summary 48
3.4 Step 4 – Assessment of Risks........ 49
3.4.1 NSDD 298........ 49
3.4.2 Risk Determination 49
3.5 Step 5 - Application of Countermeasures........ 50
4.0 MAINTAIN THE PROGRAM........ 52
4.1 Management Updates........ 52
4.2 Recordkeeping........ 53
4.3 Annual Review/Verification of Critical Information Lists 53
4.4 OPSEC Awareness........ 53
4.4.1 Briefings........ 54
4.4.2 Learning Styles........ 54
4.4.3 Activities 55
4.4.4 Concerns........ 55
4.4.5 Delivering the OPSEC Message........ 56
4.5 OPSEC Training........ 58
4.6 Summary 59
Appendix A: National Security Decision Directive Number 298 61
Appendix B: Sample OPSEC Plan 65
Appendix C: Sample OPSEC Assessment Report........ 70
Appendix D: Sample Threat Statement 86
Appendix E: Sample Website Reviews 87
Appendix F: IOSS OPSEC Program Implementation Tiers........ 88

LIST OF FIGURES

Figure 3.1. Five Steps of the OPSEC Process..14
Figure 3.2. Review and Approval Process for Information Release...20
Figure 4.1. OPSEC Poster Examples..57
Figure 4.2. Additional OPSEC Poster Examples..58

LIST OF TABLES

Table 3.1. Three Levels of Rigor in Approaching OPSEC Issues...51
Table 4.1. What information and in what venues should we publish?..55
Table 4.2. OPSEC Culture...56

ACRONYMS

COMINT	Communications Intelligence
DOE	Department of Energy
ELINT	Electronic Intelligence
FBI	Federal Bureau of Investigation
FISINT	Foreign Instrumentation Signals Intelligence
HUMINT	Human Intelligence
IMINT	Imagery Intelligence
IOSS	Interagency OPSEC Support Staff
MASINT	Measurement and Signature Intelligence
NSDD	National Security Decision Directive
NTC	National Training Center
ODFSA	Officially Designated Federal Security Authority
OPSEC	Operations Security
OA	OPSEC assessment
OSINT	Open Source Intelligence
OWG	OPSEC working group
S&S	Safeguards & Security
SIGINT	Signals Intelligence
SME	Subject Matter Expert
SPP	Strategic Partnership Programs

1.0 INTRODUCTION

This Department of Energy (DOE) Handbook provides information to assist DOE sites in the development, implementation, and evaluation of the Operations Security (OPSEC) program. Specifically, it provides information on the five-step process, which includes identifying critical information, analyzing the threat, analyzing the vulnerabilities, assessing the risks, and applying countermeasures. It also includes examples of the steps and recommendations for successful application. Internal and external resources have been referenced for additional information.

This handbook does not establish new requirements and any existing requirements are explicitly referenced from national policy or a DOE Order using the terms "must" or "shall." This handbook provides guidance to implement DOE OPSEC requirements and therefore uses the words "should" or "may."

National Security Decision Directive 298 (NSDD 298) requires that all executive departments and agencies with national security missions, and the contractors that support them, establish an OPSEC program. Application of the OPSEC process is further defined in DOE Order 471.6, *Information Security*. It should be noted that for the purposes of this document, any reference to DOE Order 471.6 will refer to the most current version. Equivalencies and exemptions from the national requirements are processed in accordance with NSDD 298 and DOE Order 251.1D, *Departmental Directives Program*.

1.1 Purpose

This handbook provides general information to assist DOE sites in developing and implementing its OPSEC program. The OPSEC program promotes operational effectiveness by helping prevent the *inadvertent* compromise of sensitive or classified U.S. government activities, capabilities, or intentions. The purpose of OPSEC is to identify, control, and protect sensitive unclassified information about a mission, operation, or activity and to deny or mitigate an adversary's ability to compromise that mission, operation, or activity.

Security programs and procedures already exist to protect classified matter. OPSEC uses information generally available to the public, as well as certain detectable activities that reveal the existence of and sometimes details about classified or sensitive information or undertakings. Such indicators may assist those seeking to neutralize or exploit U.S. government actions in the area of national security. The OPSEC program includes the development of countermeasures to deny or deter access to those adversaries.

For clarity, critical information will be spelled out throughout this document; however, there are different acronyms used by the government. Those acronyms include, but may not be limited to: CI (critical information) as used in DOE Order 471.6, CPI (critical program information), and CRINFO (critical information). OPSEC is applicable to the entire DOE complex, including all DOE elements and their contractors, OPSEC managers, safeguards and security staff, working group members, and general site personnel.

1.2 Understanding OPSEC

1.2.1 History

The underlying principles of denying an adversary information are centuries old. George Washington was quoted as saying, “Even minutiae should have a place in our collection, for things of a seemingly trifling nature, when enjoined with others of a more serious cast, may lead to valuable conclusion.”

Millennia before, Sun Tzu wrote, “If I am able to determine the enemy’s dispositions while at the same time I conceal my own, then I can concentrate and he must divide.”

OPSEC was developed as a methodology during the Vietnam War, when Admiral Ulysses Sharp, Commander of the Pacific Fleet, established the “Purple Dragon” team to determine how the enemy was able to obtain advanced information on military operations. The team realized that current counterintelligence and security measures alone were not sufficient. They conceived of and used the methodology of “thinking like the wolf,” or looking at your own organization from an adversarial viewpoint. They discovered that U.S. forces were unvarying in their tactics and procedures, and the enemy was able to make certain predictions based on that knowledge. When developing and recommending corrective actions to their command, they coined the term “Operations Security.”

In January 1988, President Ronald Reagan signed NSDD 298, which states that each executive department or agency that is assigned to or supports national security missions with classified or sensitive activities is required to create a formal OPSEC program. NSDD 298 (provided as Appendix A) establishes a national structure and describes OPSEC as “…a systematic and proven process by which the U.S. government and its supporting contractors can deny potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive government activities.” It further describes the OPSEC process, and provides guidance on the application of this process within department and agency activities.

1.2.2 Current Application

OPSEC is an analytic process designed to determine how adversaries may collect information so countermeasures can be implemented to prevent exploitation of associated critical information. The OPSEC program does not replace or lessen the importance of traditional security measures, but augments and enhances these traditional security measures by applying sound OPSEC principles.

Effective implementation of OPSEC policies and countermeasures will have a positive effect on most organizations and workplaces. Incorporating OPSEC into day-to-day planning and operations provides for early detection of concerns and makes OPSEC second nature to employees. Below are various applications of the process:

- **Day-to-Day Operations.** Routine OPSEC activities should include responses to requests (Freedom of Information Act, email, telephone calls), open source communications (including news releases, blogs, social media accounts and posts, maps, Global Positioning System location information on pictures, etc.), website reviews, awareness of employee activities, visitors to your facility, and community events (conventions, protests, open meetings).

- **Contingencies.** A contingency is a temporary period of adjustment to the normal work routine to cover some unique event. Remember, the adversary may be tipped off to a new activity by detectable and observable changes in normal daily routines. Reviewing contingencies ensures there are no changes to long-term projects that may require updates.
- **Planning.** The OPSEC program should identify activities to be considered during planning, including identification of critical information, threat assessment, vulnerabilities, risk assessment, countermeasures, and documenting the responsible individual(s) for those activities. Tracking this process allows early detection of OPSEC concerns, which can greatly minimize the damage an adversary can do.

2.0 ESTABLISH AN OPSEC PROGRAM

Because DOE has a national security mission, it is required by NSDD 298 to establish a formal organizational OPSEC program; issue, as appropriate, OPSEC policies; designate departmental and agency planners for OPSEC; and advise the National Security Council on OPSEC measures required of other Executive departments and agencies in order to achieve and maintain effective operations or activities. Additionally, DOE needs to ensure that education of individuals to the objectives, principals, and techniques of the OPSEC process is available, and provide assistance to those who should develop local formalized OPSEC programs.

As stated in NSDD 298, the OPSEC program shall have the following common features:

- Specific assignment of responsibility for OPSEC direction and implementation.
- Specific requirement to plan for and implement OPSEC in anticipation of and, where appropriate, during department or agency activity.
- Direction to use OPSEC analytical techniques to assist in identifying vulnerabilities and to select appropriate OPSEC measures.
- Enactment of measures to ensure that all personnel, commensurate with their positions and security clearances, are aware of hostile intelligence threats and understand the OPSEC process.
- Annual review and evaluation of OPSEC procedures so as to assist in the improvement of OPSEC programs.
- Provision for interagency support and cooperation with respect to OPSEC programs.

2.1 OPSEC Program Plan

The OPSEC Program is dependent on those requirements found in DOE O 471.6. An OPSEC plan for each site or facility, as determined by the governing program office, should be developed and documented accordingly (Section 2.2).

OPSEC planning requires a clear understanding of the activity’s mission and organizational plans. Early implementation of OPSEC planning helps to identify critical information to be protected throughout the lifecycle of the program. The OPSEC program must be documented and integrated into organizational activities by personnel familiar with the operational aspects of the activity in coordination with supporting counterintelligence and security activities. The local OPSEC plan(s) should identify the purpose, roles and responsibilities, implementation of the five-step OPSEC process, and assessment determinations.

This plan should establish an active and cost-effective OPSEC program for the organization. It may encompass all activities at a site or be comprised of multiple plans governing individual activities or projects. In either case, it should describe the structure and theme of the OPSEC program as well as how the program will be administered and managed.

The plan should also include:

- Identification of internal and external roles and responsibilities for other personnel who can and will support the program (see Section 2.3).
  - Appointment of an individual to be responsible for the day-to-day operations of the OPSEC program. This person is responsible for the overall program management and administration. The name of the responsible individual should be provided to the DOE Office of Security Policy (AU-51).
  - Establishment of an OPSEC Working Group(s). The working group should consist of representatives from various site programs and facilities.
  - Establishment of programmatic relationships.
    - Integrate the OPSEC program into all aspects of site operations.
    - Establish and maintain liaison with various site personnel and offices, such as Intelligence, Counterintelligence, cybersecurity, foreign visits and assignments, project managers, etc.
- Identification of information pertaining to activities, programs, facilities, and personnel requiring OPSEC protection.
- Development of the critical information list (see Section 3.1).
- Conduct of OPSEC reviews (see Section 3.1.5).
- Conduct of OPSEC assessments (OAs) (see Section 3.3.1).
- Identification of site-specific OPSEC threats not addressed by higher-level threat documents (see Section 3.2.3).
- Development and recommendation of countermeasures (see Section 3.5).
- Development and maintenance of OPSEC program files for reference and program documentation (see Section 4.2).
- Development and implementation of an OPSEC awareness program (see Section 4.4).
- Development and implementation of an OPSEC training program (see Section 4.5).
- Sharing and exchanging OPSEC-related information and products with other DOE organizations and the national OPSEC community (see Section 2.5.2).

2.2 Identification of Roles and Responsibilities

2.2.1 Site – Federal, Contractor, and Tenant Organizations

In addition to the roles and responsibilities required in DOE Order 471.6, Section 5, sites should consider identifying local roles and responsibilities that may include:

- Officially Designated Federal Security Authority.

  - Approve the security plan which includes the OPSEC plan. If it is not part of the security plan, the OPSEC plan will require ODFSA approval.
  - Approve countermeasures as appropriate.
  - Fulfill requirements and responsibilities delegated to them.
  - Provide oversight of the OPSEC program.
  - Review vulnerabilities resulting from OAs that do not require a deviation from DOE policy that results in moderate or high risk.
  - Approve equivalencies.

- Officially Designated Security Authority
  - Fulfill requirements and responsibilities delegated to them.
  - Identify individual responsible for overall OPSEC responsibilities.
  - Develop and submit deviation requests.
  - Approve the OPSEC plan and submit for inclusion in an approved security plan.

- OPSEC Managers (titles may vary by site)
  - Responsible for overall day-to-day management and administration of local OPSEC program in compliance with NSDD 298, DOE O 471.6, and as provided by law and/or contract.
  - Provide management with the information required for sound risk management decisions concerning the protection of sensitive information.
  - Develop and implement local policies and procedures.
  - Develop the knowledge base and charter for any OPSEC working groups (OWGs) established.
  - In conjunction with the DOE Office of Intelligence and Counterintelligence, develop threat information to support the OPSEC program.
  - Coordinate and communicate with other programs such as primary mission support personnel, key stakeholders, foreign visits and assignments, cybersecurity, etc.
- OPSEC Practitioner (titles may vary by site)
  - Provide support to the OPSEC manager and assists in program activities.
  - OPSEC practitioners should have the appropriate access authorization and other authorizations necessary to access information when conducting their OPSEC responsibilities.

2.3 Establish an OPSEC Working Group

OPSEC working groups are highly encouraged because of the value added to the program. As necessary, the OPSEC program office should establish one or several OWGs within their respective organizations. Normally the OWG is composed of representatives from major organizational elements (contracts, human resources, public relations, budget, operations and maintenance, etc.) to assist in identifying vulnerabilities and making recommendations for corrective action or countermeasures. Members should be selected from positions normally included in policy decision-making and have a routine relationship with a broad range of other operational and policy areas within the facility. The necessity for security clearances for OWG members should be considered when selecting members. Development of an OWG charter is encouraged to clearly capture roles and responsibilities.

OWGs should be established to assist the OPSEC program office with items such as:

- Developing and setting priorities for the program consistent with approved plans and policies.
- Assisting with the development and prioritization of the critical information list items and related indicators.
- Ensuring that OPSEC awareness briefings and materials are provided by OWG members to their group's employees and contractors.
- Reviewing and discussing the OPSEC plan and threat information on a regular basis.
- Ensuring that suggested corrective measures to mitigate vulnerabilities identified during OAs are sufficient, workable, and implemented within their organization.

2.4 Coordination and Communication

A successful OPSEC program should have a great source of relevant connections and a network to call on when needed. The OPSEC community has a proud tradition of sharing, communicating, and networking among DOE sites, with other government agencies, local law enforcement, and private contractor organizations. Networking provides a source of connections and opens the door to new ideas, solutions to problems, and professional associations.

Consulting other subject matter experts (SMEs) and OPSEC professionals provides the opportunity to network and tap into advice and expertise that would not otherwise be available. If management and budget allow, other networking opportunities and resources to consider may include: the national Interagency OPSEC Support Staff (IOSS) conference; local or regional OWGs (often sponsored by other government agencies, local law enforcement, or other DOE federal or contractor organizations); and community events, such as the local chamber of commerce meetings where information on conferences or groups that will be coming to town is available.

2.4.1 Office of Intelligence/Counterintelligence

Because OPSEC is threat driven, it is vital that the OPSEC manager or their representative establish a strong relationship and ongoing communication with the appropriate representative from the DOE Offices of Intelligence and Counterintelligence either at the headquarters or local level. Per DOE O 475.1, *Counterintelligence Program* and DOE O 5670.1A, *Management and Control of Foreign Intelligence,* information developed through Intelligence and Counterintelligence_program activities is to be shared with appropriate program offices, to include the OPSEC program. DOE O 475.1 further states the Counterintelligence Office will conduct liaison with site counterparts (e.g., security, intelligence, export control, technology transfer, technical surveillance countermeasures, OPSEC, and nonproliferation personnel) on national security matters. DOE O 5670.1A requires the Director of Intelligence to share foreign political, economic, military, or facility threat-related intelligence and counterintelligence information, as appropriate. This communication and coordination is crucial to developing a sound threat analysis. As a reminder, a threat analysis should be developed, documented, reviewed annually, and updated as necessary to include requirements stated in these directives.

2.4.2 Internal and External Organizations

OPSEC professionals typically interact with internal and external entities. This interaction is an opportunity for program staff to exchange ideas, share lessons learned, and not "reinvent the wheel" but rather learn from another organization’s success or failure. The following list may not be all-inclusive as individual sites may have additional site-specific contacts.

Internal interfaces typically include:

- Office of the Chief Information Officer
- Line personnel
- Members of OWGs
- Environmental safety and health staff
- Management teams
- Field Intelligence Elements and/or Special Access Programs personnel
- Counterintelligence
- Local Insider Threat Working Group
- Other Safeguards and Security (S&S) SMEs (e.g., Security Incident Management Program, classified matter protection and control, foreign visits and assignments, S&S training, intelligence)
- Other site working groups (threat/risk, etc.)
- Other strategic, collaborative, and initiative teams (e.g., programmatic, communications, outreach, tactical)

External interfaces typically include:

- Federal OPSEC program oversight officials
- Other DOE OPSEC professionals
- Other government agencies’ OPSEC professionals (Department of Defense, Department of Homeland Security, etc.)
- Federal, state, and local law enforcement agencies
- Members and staff from the OPSEC Professionals Society, OPSEC Professional Association, and IOSS

2.4.3 Foreign Visits and Assignments

DOE O 142.3A, Change 1 (MinChg), *Unclassified Foreign Visits and Assignments Program*, requires the site security plan to include an SME review, host and escort requirements, and that the review is documented in the Foreign Access Central Tracking System database. Optimally the OPSEC program office would serve as the security SME in the foreign visit and assignment approval process since the requested access is often associated with access to DOE facilities, programs, information, and technologies.

All foreign visit request packages should be reviewed in accordance with DOE Order 142.3A, Change 1 (MinChg), Section 4.e, and include a program office review for OPSEC concerns. These reviews should ensure that any identified risk to the government associated with access approval for each visit or assignment has been appropriately evaluated and mitigated.

This process allows OPSEC program staff, in coordination with visit hosts, to review all visit requests and implement countermeasures to mitigate the foreign visit threat to national assets.

3.0 APPLY THE OPSEC FIVE-STEP PROCESS

OPSEC procedures and requirements were formalized under the provisions of NSDD 298. OPSEC was not intended to be a replacement for security programs created to protect classified information such as physical security, information security, and personnel security, but was developed to promote operational effectiveness by denying adversaries publicly available indicators of sensitive or classified activities, capabilities, or intentions. The goal of OPSEC is to control information and observable actions about an organization's capabilities, limitations, and intentions to prevent or control exploitation of available information by an adversary. The OPSEC process involves five steps, as shown in Figure 3.1.

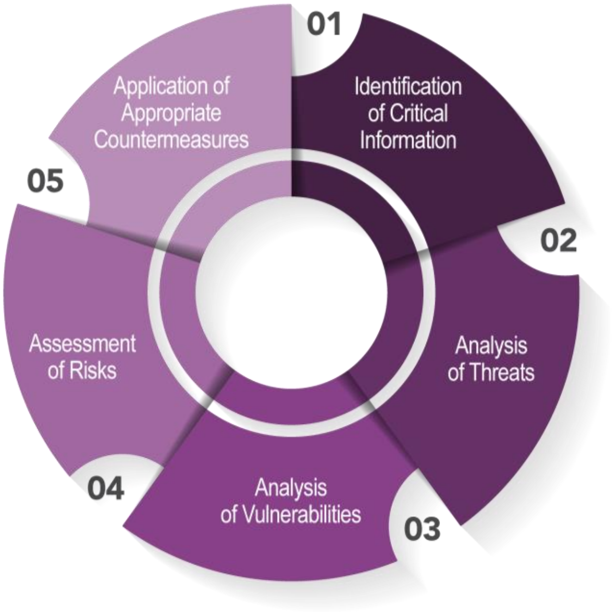
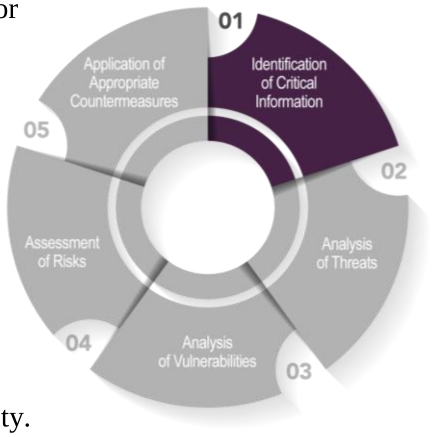

01
Identification of Critical Information
02
Analysis of Threats
03
Analysis of Vulnerabilities
04
Assessment of Risks
05
Application of Appropriate Countermeasures

Figure 3.1. Five Steps of the OPSEC Process

Although the OPSEC process is described as having five definitive steps, which are not intended to be strictly adhered to in sequential order, they should be repeated as often as needed or required. A recognized strength of the OPSEC process is that its elements are fluid, enabling the process to adapt to the particular needs of the organization. The key benefit of the OPSEC process is that it provides a means for developing cost-effective security countermeasures tailored to meet the identified threat. The process begins with an examination of the entire organization or activity to determine what exploitable but unclassified evidence of classified or sensitive activities may be acquired by an adversary through known collection capabilities. Evidence indicating sensitive activities can often be obtained from publicly available information and pieced together to derive critical information. Indicators of sensitive activities may result from routine administrative, logistics, or operational activities that are known to precede the execution of a plan or activity. Coordination and liaison with other staff and program offices is critical to developing and maintaining a good OPSEC program. Whenever possible, OPSEC managers should leverage the results of local analyses (e.g., hazards analysis, security risk assessments, vulnerability assessments) already conducted by the site in preparation for design basis threat implementation. Once identified, indicators are analyzed in terms of the known collection capabilities of an adversary. Program managers or decision-makers have the ultimate responsibility for mission accomplishment and resource management and will determine where and how OPSEC will be applied.

3.1 Step 1 – Identification of Critical Information

Critical information describes those areas, activities, functions, data, or information about an activity or facility deemed most important to protect. Looking at it from the adversary's point of view, it is the information about intentions, capabilities, or activities needed to effectively plan and impact the accomplishment of friendly objectives. It may be classified or unclassified information of a sensitive nature which may also be controlled unclassified information. The OPSEC program focuses primarily on the unclassified information adversaries can collect and analyze, and then exploit by compromising, sabotaging, or duplicating. The OPSEC process may also help determine when that information may cease to be critical in the life cycle of an operation, program, or activity.


01
Identification of Critical Information
02
Analysis of Threats
03
Analysis of Vulnerabilities
04
Assessment of Risks
05
Application of Appropriate Countermeasures

Critical information is distinguished by the detectable activities and bits of data (indicators) that can be pieced together to deduce the actions, capabilities, or intentions of organizations of these sensitive programs and activities. Classified information or activities are normally protected by traditional security programs (e.g., personnel, information, and physical security); the scope of OPSEC efforts supports or enhances those traditional security programs.

Critical information is what an adversary views as valuable. Critical information that is most accessible to the adversary is found in support activities such as administration, budgeting, communications, logistics, proprietary information, Official Use Only (OUO), Export Controlled Information (ECI), or personally identifiable information (PII); however, it does not need to be marked as such to be an OPSEC concern. Even seemingly insignificant information may be valuable to an adversary's collection efforts and be a part of a larger picture. Prevention or delay of the adversary's ability to collect critical information will help ensure mission success. The inadvertent release of marked or unmarked critical information can cause harm to sensitive programs, activities, or resources, including people.

3.1.1 Development and Prioritization of Critical Information List

The critical information list is a compilation of critical information topics. Sites often have one critical information list but remote sites or centers may maintain their own. It is necessary to share this information for program and assessments. Critical information lists can often contain classified information so a classification review should be conducted whenever the list is developed or modified.

When developing the critical information list, the OPSEC manager in coordination with the OWG and SMEs should attempt to answer the question, "If I were tasked to find out information about my facility, what would I want to know and where would I look for it?" The "what" would be the critical information and the "where" would be the indicators or pathways that lead to the critical information. Once identified, the items on the list are prioritized. This process includes weighing the relative sensitivity of the critical information identified against the threat.

The critical information list and indicators should be approved by senior management and reviewed on a continuing basis to ensure it conforms to changes in technology and includes development of new programs and projects.

3.1.2 Elements of Critical Information

Critical information includes specific facts vitally needed by adversaries about intentions, capabilities, operations, and other activities that allow sites to plan and act effectively so as to guarantee failure or unacceptable consequences for mission accomplishment.

The following are examples of generic critical information. This is not a complete listing of critical and sensitive information, but provides some idea of the type of information included on the list.

- Date of planned tests and activities
- Test results
- Critical procurement items
- Shipment of nuclear material or devices
- Protective force capabilities and vulnerabilities
- Programmatic activities and capabilities related to the emergency response program
- New technology applications
- Certain aspects of treaty verification
- Procurements
- Vendors

3.1.3 Indicators and Pathways

Indicators include any detectable activities (collectible or observable) and/or information that, when examined in isolation or in conjunction with other data, point to vulnerabilities or critical information items that can be exploited by an adversary. Indicators and pathways are the means by which the adversary can obtain an organization’s critical information. The adversary is primarily looking for three categories of indicators or pathways into friendly operations: patterns, deviations, and signatures. Patterns are repetitive activities that show sequence and timing of how a person or organization conducts operations. Deviations are activities that are not part of a person’s or organizations normal conduct of operations (e.g., special or unusual events). Signatures are the signs or evidence that expose or point to the presence of critical information.

Individuals and organizations exhibit several types of patterns in their day-to-day activities. Customs refer to those activities that are normally conducted for certain events. For example, it is customary for the leader of an organization to call a meeting of top-level managers for a dignitary or notable public figure’s visit. Routines are those daily activities that a person or organization performs during normal operations. Shift change for the protective force is a routine activity that is conducted at prescribed times and done according to standard operating procedures. Habits refer to individual activities that a person engages in throughout the day. For example, most employees take the same route to and from work every day.

Through surveillance and observation, the adversary can discern the customs, routines, and habits of an individual or organization that will enable the adversary to predict and anticipate friendly actions.

Deviations are those activities that persons or organizations engage in when performing tasks in support of special or unusual events. An example of a typical deviation is the behavioral change that occurs in response to an accident or workplace emergency. While deviations are a disruption of a person's or organizations normal pattern of activity, they nevertheless provide valuable data to the adversary. Deviations give insight into how the person or organization performs when the unexpected happens.

Signatures or indicators—the two terms are used synonymously—are data derived from friendly actions and open source information that adversaries can exploit to reach conclusions or estimates of friendly activities, capabilities, or intentions. A typical example of a signature is the sudden increase in activity and the presence of known S&S personnel that usually precedes the conduct of a force-on-force exercise. By recognizing and interpreting such a signature, the adversary can predict or anticipate that this activity may be an opportunity to observe protective force tactics, techniques, and procedures. Once the adversary has gathered sufficient data to identify a person's or organization's patterns, deviations, and signatures, the adversary has developed a profile on that person or organization. That profile will enable the adversary to delve deeper into friendly actions, capabilities, and intentions.

The following is not a complete list of signatures, but provides generic indicators that can lead to the critical information:

- Work schedules
- Shipping requests or announcements
- Meeting minutes or notes
- Various reports, such as monthly and annual reports
- Scope of work documents
- Organization charts
- Unusual occurrence reports
- Purchasing requests
- Travel requests and trip reports
- Project or engineering drawings or blueprints
- Cost plus award fee or performance-based drafts and reports
- News releases
- Progress reports
- Published articles
- Corporate newsletters
- Emergency plans and procedures
- Budget or financial documentation
- Employee suggestions or grievances
- Standard operating procedures
- Environmental impact statements
- Position vacancy announcements
- Operating manuals
- Safety reports
- Recruitment postings

- Quality assurance notes
- Information contained on web pages
- Social media sites
- Un-erased whiteboards
- Direct observation of activities, exercises, and tests

There is no specific requirement on how to format the critical information list and supporting indicators. A suggested format includes the priority, critical item of information, and elements of critical information and indicators associated with the item, written in a clear, concise manner.

3.1.4 OPSEC Reviews

An OPSEC review is a broad scope review of a specific facility, program, or activity to ascertain whether critical information exists and determine the level of OPSEC support required. This review is usually coordinated with the OPSEC manager or designated OPSEC representative. These reviews are management tools to identify critical information and aid in subsequent steps. An OPSEC review may result in simply documenting that no further OPSEC support is required or it may determine that additional OPSEC support should be established. Those additional support activities may include: OPSEC assessments; consultations; additions to or creation of critical information lists; determination of indicators, vulnerabilities, or risks; development or modification of OPSEC plans, etc. The OPSEC review should be conducted early on as part of the planning process related to construction or changes in mission scope. DOE O 471.6 requires a review and update of OPSEC program critical information documentation "as necessary to reflect current assets, threats, operations, and other relevant factors."

Reviews may indicate that a facility, program, or activity warrants that it be included on the regular schedule for OAs. The review should be conducted whenever one of the following conditions occurs:

- New construction is planned for a facility that will process or store classified or sensitive information or matter. New construction may consist of the addition, demolition, or modification of structures, systems, or components for both buildings and infrastructure that affect the security posture or security interest of a building or infrastructure.
- New sensitive activities are initiated or existing programs incur significant changes. Sensitive programs present a target to adversaries including but not limited to: classified, sensitive, and unclassified programs, and those programs that fall into applicable governmental sensitive technology lists. Sensitive compartmented information facilities (SCIF) and special access programs (SAP) are considered sensitive programs. Significant changes that affect OPSEC critical and sensitive information include but are not limited to: new activities, funding, staffing, procurements, vendors, new technology, deliverables, Strategic Partnership Programs (SPP) footprint, scope, classification, and security area types (new or moves).
- A sensitive program or activity has not been the subject of an OA for the preceding 3 years.

3.1.5 Public Release Review

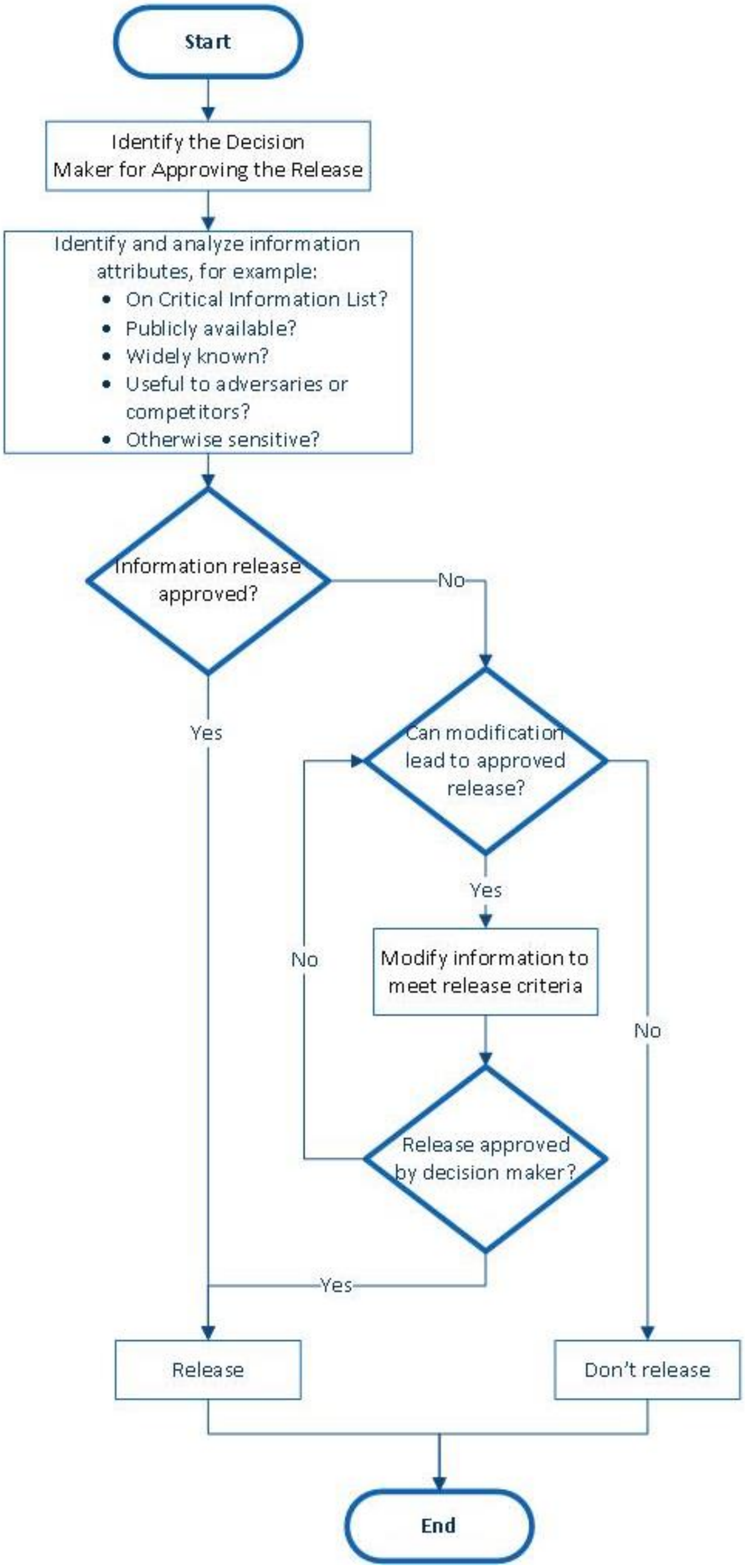
According to DOE O 471.6, "Information generated by or for the Federal Government and being placed on any website or otherwise being made available to the public must not contain critical information unless authorized by the Officially Designated Federal Security Authority (ODFSA)."

Before DOE employees, contractors, or subcontractors post government information to a personal or non-DOE website it should also be reviewed for the same concerns (see Appendix E). The review process should include a multilayer review to ensure suitability of the information for worldwide public release. This applies to news releases, promotional materials, technical publications, RFPs, personal resumes, etc.

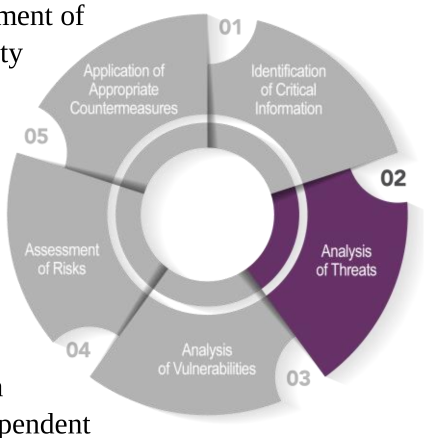
Automated analysis tools can be used to assist in the review of information to determine if it is appropriate to release it to the public. Certain categories of unclassified information are generally recognized as unsuitable for public release. These include, but are not limited to, controlled unclassified information such as Official Use Only (OUO), Unclassified Controlled Nuclear Information (UCNI), personally identifiable information (PII), protected Cooperative Research and Development Agreements (CRADA), and export control sensitive subjects. Due to the diversity of information within DOE, a robust review and approval process should be conducted using the following evaluation factors for determining suitability for release of information to the public (Figure 3.2):

- **Sensitivity**. If the information is released to the public, it should not reveal or identify sensitive information, activities, or programs.
- **Risk**. Information that may be used by adversaries to the detriment of employees, the public, the department, or the nation should not be approved for release. This determination should be based on sound risk management principles focused on preventing potential adverse consequences.

Figure 3.2. Review and Approval Process for Information Release


Start
Identify the Decision Maker for Approving the Release
Identify and analyze information attributes, for example:
• On Critical Information List?
• Publicly available?
• Widely known?
• Useful to adversaries or competitors?
• Otherwise sensitive?
Information release approved?
No
Yes
Can modification lead to approved release?
Yes
Modify information to meet release criteria
No
No
Release approved by decision maker?
Yes
Release
Don't release
End

3.2 Step 2 – Analysis of Threats


01
Identification of Critical Information
02
Analysis of Threats
03
Analysis of Vulnerabilities
04
Assessment of Risks
05
Application of Appropriate Countermeasures

The second step in the OPSEC process is the identification and assessment of the threat. Threat analysis consists of determining the adversary's ability to collect, process, analyze, and use information. The objective of threat analysis is to know as much as possible about each adversary and their ability to target the organization. It is especially important to tailor the adversary threat to the actual activity and, to the extent possible, determine what the adversary's capabilities are with regard to the specific operations of the activity or program. Coordination and liaison with Intelligence, Counterintelligence and other intelligence and law enforcement agencies may assist in the gathering of threat information. In some cases, there are local program offices, and in others there are not, so the OPSEC Manager may be dependent on local agency and law enforcement for information sharing.

Specific threats vary from one DOE site to another and from one program to another with direct relevance to the types of operations conducted. DOE O 470.3C, *Design Basis Threat*, identifies and characterizes potential adversary threats to DOE programs and facilities and should be the baseline for the development of the facility’s OPSEC threat statement (see Appendix D for an example). The purpose of the threat statement is to identify the potential threats to local site programs, facilities, information, resources, and activities. Through collaboration with the local field intelligence elements, DOE senior counterintelligence officer, local law enforcement, etc., the OPSEC manager should leverage the results of analyses (e.g., hazards analysis, security risk assessments, vulnerability assessments) already conducted by the site in preparation for design basis threat implementation.

Many countries target their efforts against the United States and DOE to obtain critical information serving their interests or goals. Adversary strategies continue to focus on economic and defense-related information, which includes technology design, use, and innovation. The threat to advanced technology can cause loss of information that adversely affects the ability of the United States to compete worldwide or protect customers.

Innovation is the engine that drives American industry. Through a multi-phased acquisition process, government partners with industry to apply innovation against challenges to the national objectives. By design, government acquisition processes must maintain a level of transparency to ensure economic competitors and citizens that the business of government is conducted fairly and reasonably and to enhance collaboration critical to the realization of advanced technological breakthroughs.

Within this framework, the National Counterintelligence and Security Center, formerly called the Office of the National Counterintelligence Executive, reports (NCIX 2009):

> *“… a wide variety of foreign entities continued to try to illegally acquire US technology, trade secrets, and proprietary information” and, “…the most heavily targeted sectors across all [government] agencies included [unclassified and classified] information on aeronautics, information systems, lasers and optics, sensors, and marine systems.”*

In 2005, the Federal Bureau of Investigation (FBI) arrested a Kentucky maintenance mechanic for selling more than 800 blueprints of his employer's innovative equipment for making liquid crystal displays to a foreign-based rival, leading to a conviction of conspiracy to commit trade secret theft,. The blueprints were worth an estimated $100 million. The aggregation of unclassified data over time and the trusted insider threat nearly resulted in a catastrophic financial disaster for the company. "Stealing trade secrets is worse than stealing money from a company. It's like robbing a company's future," (NCIX 2009).

The General Accounting Office reports the cost to the Department of Defense of schedule delays [independent of cause] in 95 weapons systems programs in 2007 was $4.9 million per day. The loss of critical information can lead to unnecessary systems redesign. Effective OPSEC helps avoid redesign and contributes directly to a program's bottom line (NCIX 2009).

"Developing new technologies ensures we remain competitive in modern economic and military arenas, but only if we protect the fruits of our labor," (NCIX 2009). OPSEC provides a cost-effective, repeatable risk analysis process for acquisition program managers to reach program goals and attain an optimal level of transparency through the systematic protection of critical information.

Government acquisitions involve advanced research and development activities associated with new technologies, production of critical military equipment or logistics activities in direct support to sensitive or classified government activities. The effective protection of critical information is at the heart of maintaining our nation's technologic advantage and is key to the ability of the government, academia, and industrial communities to provide superior tools for achieving the nation's strategic objectives.

The world is constantly changing and the same is true of the threat. As a world leader, the United States is a principal target for the exploitation of its technology and the acquisition system and contractors, often performing at the leading edge of technology, make an enticing target for an adversary.

During the Cold War era the threat to the United States was generally static and consisted primarily of the Soviet Union and its allies. Today the threat derives from a list of well-known nation-states and a dynamic list of economic competitors and terrorist organizations with only oblique ties to nation-states. Detailed information concerning specific adversary capabilities is a necessary input to the OPSEC process and may be obtained from U.S. Intelligence Agencies or local law enforcement organizations. This type of information is always a critical component of a well-written OPSEC plan.

3.2.1 Intelligence Cycle

For the OPSEC manager an understanding of the intelligence cycle is helpful in considering potential threats and ways to counter these threats. A brief explanation of the intelligence cycle and the principal techniques used to collect classified and unclassified information of a sensitive nature (which may also be controlled unclassified information) is provided in this section. The following definitions should be considered in the development of any threat statement:

- **Threat.** A person, group, or movement with intentions to use extant or attainable capabilities to undertake malevolent actions against DOE interests. The capability of an adversary coupled with his/her intentions to undertake any actions detrimental to the success of program activities or operation.

- **Threat Analysis.** A process in which information about a threat or potential threat is subjected to systematic and thorough examination to identify significant facts and derive conclusions.
- **Threat Assessment.** A judgment based on available intelligence, law enforcement, and open source information of the actual or potential threat to one or more DOE facilities/programs.

The intelligence cycle is the process through which information is obtained, produced, and made available to decision makers. In depicting this cycle, the U.S. Intelligence Community also uses a five-step process.

1. **Planning and direction** involves the management of the entire intelligence effort, from the identification of a need for data to the final delivery of the product to the consumer. The process consists of identifying, prioritizing, and validating intelligence requirements, translating requirements into observables, preparing collection plans, issuing requests for information collection, and producing, disseminating, and continuously monitoring the availability of collected data. In this step, specific collection capabilities are tasked based on the type of information required, the susceptibility of the targeted activity to various types of collection activity, and the availability of collection assets. Examples of questions an adversary might want to know include: What technologies is the United States investing in and at what levels? What is the status of a particular technology development and when might it be deployed? What is a particular corporation's marketing strategy for a newly developed product(s)? Where are the technical weaknesses in a new product?
2. **Collection** includes both acquiring information and provisioning that information to processing and production elements. The collection process encompasses management of various activities including developing collection guidelines that ensure optimal use of available intelligence resources. Intelligence collection requirements are developed to meet the needs of potential consumers. Based on identified intelligence requirements, collection activities are given specific taskings to collect information. These taskings are generally redundant and may use a number of different intelligence disciplines. Tasking redundancy ensures that the failure of a collection asset is compensated by duplicate or different assets capable of answering the collection need. The use of different types of collection systems contributes to redundancy and allows the collection of different types of information that can be used to confirm or disprove potential assessments. Collection operations depend on secure, rapid, redundant, and reliable communications to allow for data exchange and to provide opportunities for cross-cueing and tip-off exchanges between assets. Once collected, information is correlated and forwarded for processing and production. Internet research might reveal the development of a new leading-edge technology at a corporation (open source intelligence or OSINT), an employee of a corporation may inadvertently reveal the corporation's intent to market the technology to a U.S. government client (human intelligence or HUMINT), and intercepted telephone conversations between a sales representative and government personnel may reveal the level of interest in the technology (signals intelligence or SIGINT). Independently, the information gathered may not provide a great deal of insight into U.S. government intentions; however, the aggregation of discreet parcels of unclassified information, like pieces of a puzzle, may be used to form the basis of an answer to an adversary's questions.
3. **Processing** is the conversion of collected information into a form suitable for the production of intelligence. Incoming information is converted into formats that can be readily used by analysts in producing intelligence. Processing may include such activities as translation and reduction of intercepted messages into written format to permit detailed analysis and comparison with other information. Other types of processing include video production, photographic processing, and correlation of information collected by technical intelligence platforms. For example, OSINT may

require additional validation through research, HUMINT sources require debriefing, and SIGINT often requires technical processing or translation before final evaluation, analysis, and interpretation. The speed with which processing occurs affects how quickly an adversary may be able to provide its leadership intelligence about U.S. intentions and capabilities.

4. **Production** is the process of analyzing, evaluating, interpreting, and integrating raw data and information into finished intelligence products for known or anticipated purposes and applications. The product may be developed from a single source or from all-source collections and databases. To be effective, intelligence production must focus on the consumer's needs. It should be objective, timely, and accurate. As part of the production process, the analyst must eliminate information that is redundant, erroneous, or inapplicable to the intelligence requirement. As a result of the analytical effort, the analyst may determine that additional collection operations are required to fill in gaps left by previous collection or existing intelligence databases. The final intelligence product must provide the consumer with an understanding of the subject area and draw analytical conclusions supported by available data. Examples of analysis of acquisition-related information may include consideration of the source of the data (e.g., the vice president of marketing at a known government contractor, postings on corporate websites, and news reports), the validity of the data (e.g., how many sources are reporting the information), and does the data make sense when considering previously revealed information.
5. **Dissemination** is the conveyance of intelligence to the consumer in a usable form. Intelligence can be provided to the consumer in a wide range of formats including verbal reports, written reports, imagery products, and intelligence databases. Dissemination may be through physical exchanges of data and/or interconnected data and communications networks. Once the intelligence has been communicated and absorbed, additional intelligence requirements may be levied by the adversarial leadership and the intelligence cycle is then repeated.

OPSEC program personnel should understand the intelligence cycle for three reasons. First, they must be aware of the range of threats that confront the program or they will not be able to implement countermeasures to deny the adversary access to data that may provide sensitive information. Second, knowledge of the intelligence cycle allows the OPSEC program to develop protective measures to thwart adversary collection activities. Knowledge of adversary intelligence planning derived through U.S. intelligence collection allows the OPSEC manager to determine if their facility, operation, or program is targeted, or is likely to be targeted, by a particular adversary. Knowledge of an adversary's collection methods and patterns allows the development of effective countermeasures. Third, knowledge of the adversary's analytical biases can be used to develop programs that deceive the adversary by confirming erroneous perceptions.

Access to intelligence information may be highly classified and require a "Q" access authorization (and perhaps even Sensitive Compartmented Information (SCI) access).

3.2.2 National Threats

The design basis threat is a statement of the baseline threat to DOE sites, facilities, programs, information, and activities. In the development of this threat statement, site-specific geographical, environmental, or other unique facility or location characteristics are not considered. It is understood that local threat statements, taking into account site- and region-specific conditions, will be developed to supplement the design basis threat. The following definitions describe adversary groups addressed in the design basis threat:

International Terrorists. Persons or groups who transcend U.S. national boundaries to plan or engage in violent acts dangerous to human life and property. The objective of this adversary can vary widely to include loss of life; damage to infrastructure and property; or to obtain, destroy, or use a nuclear weapon or special nuclear material, radiological material, chemical, or biological agents.

Domestic Terrorists. Persons or groups who are U.S. citizens who plan or engage in violent acts dangerous to human life and property. This adversary would include homegrown violent extremists. The objective of this adversary can vary widely to include loss of life; damage to infrastructure and property; or obtain, destroy, or use a nuclear weapon or nuclear material, radiological material, or chemical or biological agent.

Criminals. An individual or group who obtains and/or seeks to use government property, classified and/or Controlled Unclassified Information or material, or nuclear material for the purpose of gaining economic advantage; or alters data maintained by DOE; steals; embezzles government funds; or commits contract fraud. Can be employee(s) and/or person(s) unaffiliated with the DOE, and encompasses the "criminal actor or group" as well as the financial or "white collar" criminal.

Psychotics. Psychotic illnesses alter a person's ability to think clearly, make good judgments, respond emotionally, communicate effectively, understand reality, and behave appropriately. This individual can be an employee (i.e., insider) or a member of the community (i.e., outsider). The objectives of the psychotics can vary based on the individual's mental and emotional state of mind and specific experiences.

Disgruntled Employee. An individual who has become malcontent or disillusioned with the workplace environment for any number of reasons such as feeling overworked, underpaid, unappreciated, passed by for promotion, or other disagreements/conflicts with management or coworkers. This individual could resort to violence and/or other malicious or vindictive acts against persons and/or property. This individual can be either an existing or former employee of the organization.

Activists. Also referred to as single-issue extremists, they may include violent activists who commit malevolent acts (violent, destructive, or disruptive) in opposition to DOE programs and are driven by ideological, ecological, political, or economic concerns, in violation of federal, state, and/or local laws. The category of violent activists *does not include* lobbyists, pressure groups, nonviolent demonstrators, and others opposed to the development and use of nuclear energy, nuclear weapons, or other DOE or federal programs, who engage in lawful actions to bring about a cessation of these activities.

Threat Identification Resources. The national threat includes nations, groups, and individuals who seek to harm the United States. The rapid changes in the global political and economic climate have produced a number of significant changes in the perception of threat at the national level. Several valuable sources of threat information, along with additional awareness materials, can be found at https://www.dni.gov. Items of interest found on the website include but are not limited to:

- *National Counterintelligence Strategy of the United States of America 2016* was developed in accordance with the Counterintelligence Enhancement Act of 2002. The strategy sets forth how the

U.S. government will identify, detect, exploit, disrupt, and neutralize foreign intelligence entity threats. It provides guidance for the counterintelligence programs and activities of the U.S. government intended to mitigate such threats. Each U.S. government department and agency has a role in implementing this strategy in the context of its own mission and through application of its unique responsibilities and authorities.

- *National Insider Threat Task Force* (NITTF) *Fact Sheet*. The task force was established after the WikiLeaks release of thousands of classified documents through the global media and internet. Its mission is to deter, detect, and mitigate actions by employees who may represent a threat to national security by developing a national insider threat program with supporting policy, standards, guidance, and training.
- *Annual Report to Congress on Foreign Economic and Industrial Espionage*, produced by the National Counterintelligence and Security Center, is concerned with economic and industrial espionage activities against the United States. The report notes that "many foreign countries, including some traditional U.S. allies, continue their attempts to acquire U.S. trade secret information and critical technologies for military and commercial application, through both legal and illegal means." These reports make the following important points (NCIX 2009):
  - Some of our traditional allies, as well as our traditional adversaries, are actively engaged in collecting our information for both military and economic purposes.
  - The collector does not have to be an intelligence agent. More and more non-intelligence personnel such as foreign industry representatives, students, researchers, scientists, and foreign national "insiders" working with U.S. firms are engaged in collection activities.
  - The preferred method of operation is to collect information using legal methods. This refers to the collection of open source information, whether it is found in the news media, reported on television, contained in organizational or other publications, or posted on the internet. Because there are no laws against the collection of open source information, the only recourse is a careful review of information for its sensitivity before it becomes an open source.

3.2.3 Site-Specific Threats

The OPSEC statement of threat moves from the national to the local level and goes beyond the design basis threat by documenting the real and potential threats to a particular DOE facility or site. It lists threat types and threat operating assumptions. Local information should be used to adapt the general statements from national-level assessments to provide a comprehensive assessment of the local threat situation. The local OPSEC threat assessment should systematically address each category of potential adversary in terms of four key question areas:

1. What interest would this group have in your facility? Has it demonstrated any direct interest (e.g., by visits, demonstrations, inquiries)? Has it shown concerns for your facility by attacks on U.S. government offices or thefts from technical libraries?

2. Does this group have any known or presumed information requirements associated with your facility? How significant would these requirements be? How attractive a target would your facility be for this adversary?

3. What general information collection capabilities has this particular group demonstrated? Are any of these capabilities pertinent to your facility?

4. Is any element of this group physically located in your area (e.g., a consulate, a commercial office, a local chapter)? If so, what does it do? Has it engaged in known information collection activities focused on DOE? Are there potential sympathizers (e.g., students, ethnic groups) in your area? Has the group sponsored any activities in your area such as rallies or exchange visits?

When considering whether or not a local threat exists, there are certain assumptions that should be made.

- Our adversaries are at least as intelligent as we are.
- When adversaries visit or access any facility or location for any reason, they are collecting information of some intelligence value.
- Foreign visitors and assignees, particularly those from sensitive countries, may receive pre-visit collection briefings from their intelligence services.
- Most foreign visitors and assignees may be debriefed by their intelligence agencies in some fashion upon their return.
- Adversaries will collect intelligence-valued information by any method.

Sources of information for local threats include local offices of national organizations such as the FBI, local and state law enforcement agencies, other local organizations such as the chamber of commerce, both national and local news media, and any local military intelligence offices.

Once a local OPSEC threat statement is developed, it can be put to three general types of use:

1. Analysis of OPSEC vulnerabilities, risks, and countermeasures
2. General orientation and OPSEC awareness programs
3. Specific elements on threat details pertinent to their activities (e.g., protective forces or personnel associated with a specific sensitive program).

External websites and additional resources that can aid the OPSEC manager with development of a local threat statement include:

- FBI Internet Crime Complaint Center – www.ic3.gov
- Center for Development of Security Excellence – www.cdse.edu
- Department of Homeland Security (DHS) – www.dhs.gov
- Digital.gov – www.digital.gov
- Federal Trade Commission (FTC) – On Guard Online and "Identity Theft" – www.consumer.ftc.gov
- Stay Safe Online Resources – www.staysafeonline.org
- U.S. Computer Emergency Readiness Team – www.us-cert.gov

3.2.4 Collection Techniques

Several collection techniques are used by adversaries to acquire information concerning the United States, including HUMINT, SIGINT, imagery intelligence (IMINT), measurement and signature intelligence (MASINT), and OSINT. Each of these disciplines is used by adversaries against the United States to some degree. Most nations, and many subnational and private organizations, have HUMINT capabilities they use to collect data on their adversaries and competitors. While these are not the only methods adversaries use, they are the ones most often used against our facilities and will be discussed in more detail in this handbook.

Intelligence organizations use IMINT, SIGINT, and MASINT to gather data. These collection capabilities, however, are often limited by the technological capabilities of the intelligence organization. Historically, less technologically capable nations have been unable to gain access to information; however, this situation is changing. SIGINT technologies are proliferating throughout the world and are being sold by a wide variety of suppliers to nations that are known adversaries of the United States. Imagery is becoming more readily available to nontraditional adversaries as commercial imagery products that approach the quality of intelligence collection systems become available for sale.

Most, if not all, results from critical information collections are highly classified and require individuals requesting this information to have the appropriate security clearances and storage facilities/systems. Open source collection becomes a greater threat as more information is electronically accessible. All personnel should be aware of the potential for open source collection against their activities and should ensure that protective countermeasures are developed to prevent inadvertent compromise of program activities through publication of data in publicly available media.

3.2.4.1 Imagery Intelligence

The products of imagery and photographic interpretation processed for intelligence use are referred to as IMINT. Imagery collection involves a broad spectrum of imaging techniques ranging from highly sophisticated satellite systems to handheld box cameras. Sensitive activities, equipment, or materials are often visible at DOE facilities. In many instances, publicly accessible areas provide unauthorized persons an unrestricted view of such activities, equipment, or material—often from vantage points outside the facility, such as high terrain, nearby buildings, or other structures. Unrestricted air space over or near most DOE facilities also provides viewing opportunities. It is important to note that what can be viewed can also be imaged.

The imagery threat is of increasing concern because of the ready availability of high-quality pictures. Not only do some foreign governments and intelligence services have and use the capabilities of satellite imagery, but several sell it commercially. In fact, some U.S. government agencies will, for a price, provide high-altitude aerial photography and other imagery of much of the country.

When applicable, OPSEC plans should have a section or annex describing actions to identify and counter imagery collection from air- and space-borne platforms. This portion of the plan must demonstrate how the facility will assess possible vulnerabilities by identifying distinctive physical signatures and determining vulnerable patterns of operation(s). It may be a part of the OPSEC plan or a separate standalone document.

IMINT provides adversary intelligence services with an extremely valuable collection tool, especially during system research, development, and testing stages. Capabilities, including status of the system, production rates, new initiatives, new facilities, etc., can be derived from operational activities that can be imaged. It is suggested that OPSEC managers obtain ground, airborne, and satellite imagery of their facility and, in conjunction with the OWG, perform an analysis of the imagery threat.

A further consideration related to imagery collection is the Open Skies Treaty. Flights over facilities are authorized by the treaty and require the careful consideration of OPSEC managers. Understanding the capabilities of all types of imaging systems, and the threat they represent when used in combination, is critical to the OPSEC threat analysis process.

Overflight collection under the Open Skies Treaty could result in the compromise of sensitive information. Aerial observation of special nuclear material movements, exercises, industrial plant configurations or activities, outdoor testing, protective force deployments, or storage of equipment could give foreign countries direct or indirect insight into DOE and its contractors' capabilities and readiness, beyond that which the U.S. government is prepared to disclose.

OPSEC should also be considered in foreign visits and assignments (FV&A). These assignments may have foreign nationals fly over host sites for training purposes or walk through highly sensitive work spaces in the performance of their work. Imagery collection is not confined to cameras and sensor equipment, it can be collected mentally. Careful consideration to OPSEC is vital in preventing disclosure of sensitive items or activities.

3.2.4.2 Human Intelligence

Simply stated, HUMINT is intelligence information derived from or collected by human sources. A human source is defined as "a person who wittingly or unwittingly conveys by any means information of potential intelligence value." HUMINT may be collected by members of diplomatic or trade missions; scientific, cultural, or technical exchange personnel; members of onsite inspection teams; persons visiting the United States as part of a commercial tour group or as individual tourists; merchant seamen traveling throughout the country while their ship is visiting a U.S. port of call; members of criminal elements; or well-meaning (or not so well-meaning) activists. It can also be collected by the classic intelligence agent or spy. While technical collection means (the other collection disciplines) provide very valuable information, there are instances in which HUMINT operations provide details, or pieces of the puzzle, that are not available through other sources.

Attendance at technical symposia, trade shows, and educational seminars can also provide useful HUMINT. There is also reason to believe many adversaries exploit the numerous commercial databases available both to obtain leads and to collect voluminous amounts of information related to areas they deem of specific interest. Such databases and many other open sources provide targeting information for use by the collection manager in directing the continuing spin of the intelligence cycle.

OPSEC programs should include discussions of HUMINT in local awareness training. Many have found the local FBI or the DOE Counterintelligence office are willing to provide excellent briefings on the subject.

3.2.4.3 Signals Intelligence

SIGINT is the composite of data and information from electromagnetic sources that is collected, processed, and analyzed. SIGINT is defined as intelligence information derived from signals intercept comprising either individually or in combination all communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT), however transmitted. Telemetry intelligence, (TELINT) as a subset of FISINT, is a very specialized field of direct concern to only a few DOE facilities. The same can be said for ELINT, which generally concerns collection of radar and other electronic signals. COMINT, however, is a concern throughout most of DOE. Modern electronic equipment or collection hardware provides any intelligence collector the potential to systematically listen to clear text radio and telephone microwave transmissions.

Historically, the threat of SIGINT collection was from the most sophisticated adversaries, such as the former Soviet Union and the People's Republic of China. Such adversarial threats continue to exist, albeit from nation states such as the Russian Republic (the Russian SIGINT site at Lourdes, Cuba, continues in operation and shows no signs of being closed) and quite probably remnants of the former East European Bloc, not to mention some of the nations of the world deemed "friendly" to the United States. Advances in communication electronics, microchip design, computers, and related technologies have resulted in the proliferation of equipment capable of SIGINT collection. Most of that equipment is readily available, at reasonably low cost, through numerous retail outlets throughout the country. The ability to easily obtain such collection hardware has provided less sophisticated adversaries with the capability to conduct SIGINT and simultaneously broadened the SIGINT threat spectrum for DOE.

In explaining the SIGINT threat to the workforce, it may be useful to point out that for an adversary, SIGINT can add countless up-to-the-minute details that are not otherwise available. It can also provide information on associations and linkages, which is valuable to the intelligence analyst. Because SIGINT is passive and unobtrusive, it is difficult to impress the significance of the threat upon the workforce. Personnel often accept the fact that an adversary may be capable of intercepting millions of transmissions daily; however, they find it hard to believe that an intelligence analyst could actually find their specific conversation. Providing those personnel knowledge of the capabilities of modern SIGINT equipment can help them understand how it happens. The following are some suggested facts to include in that education or awareness effort:

- Sophisticated intercept systems can pick up microwave and satellite transmissions hundreds of miles away from the intended receiver. Microwave transmissions and even walkie-talkie communications can carry far beyond the intended recipient and in some instances beyond U.S. borders, while satellite downlinks can be received anywhere within a "footprint" or an area that may be hundreds of miles in diameter.
- Scanners can continuously sweep specific frequency bands and automatically lock on active frequencies, and then voice-activated recorders operate only when a channel is active.
- Broadband recorders can automatically record a number of frequencies simultaneously (e.g., several selected channels in a telephone microwave transmission).
- Recordings can be screened by automatic processing equipment that extracts transmissions of key intelligence interest based on parameters set by an analyst. For example, this processing can extract all calls or FAX transmissions to designated telephone numbers. Sophisticated processing can search for key words or phrases, such as "tritium" or "Project Alpha," and pull out conversations containing them. This is the modern equivalent of using a magnet to find the needle in the haystack.
- Analysts actually examine in detail only those transmissions that have been preselected as likely to contain items of interest.
- Recordings are often maintained in archives and can be screened after the fact. When an analyst finds a new program involving certain people, materials, and designators, months or years of previously intercepted communications can be processed to extract pertinent information.
- Articles often appear in national and local media relating instances of the use of intercepted communications. Such information is very useful in impressing upon the workforce the fact that such things can and do happen.

3.2.4.4 Measurement and Signature Intelligence

Effluent streams could be a target for MASINT in an attempt to identify raw materials used in production activities; however, it is a relatively arcane collection discipline and only a limited number of nations have access to MASINT collection capabilities. Local OPSEC programs should include consideration of the threat of MASINT collection against their facilities. If that threat is deemed sufficient to place sensitive information at risk, countermeasures should be implemented.

3.2.4.5 Open Source Intelligence

OSINT is successful in targeting the United States because of the openness of American society. Technical and professional journals are often lucrative sources for information concerning government and commercial activities. The growing number of online databases has increased the capacity of adversaries and competitors to develop tailored data products on U.S. government and industry activities by permitting them to review large quantities of information in a very short time. Search parameters used for these databases can be structured to extract only pertinent information for analysis.

OSINT involves the use of materials available to the public. Some analysts have estimated that the Former Soviet Union derived up to 90 percent of its intelligence from open source information. With the proliferation of electronic databases, it has become easier to collate large quantities of data and structure information to meet the needs of the adversary collector. Open sources can often provide extremely valuable information concerning an organization’s activities and capabilities. Frequently, open source material can provide information on organizational dynamics, technical processes, and research activities not available in any other form. When open source data are compiled, it is possible to derive classified data or trade secrets. This is particularly true in the case of studies published in technical journals. A significant understanding of research and development efforts can often be derived by analyzing journal articles published by different members of a research organization.

Finally, open source information is generally very timely and may be the only information available in the early stages of a crisis or emergency. Screening of open source material is often an early phase of an intelligence collection operation. The openness of our society is conducive to adversary collection and many collection requirements can be satisfied by exploiting readily available sources. Those sources include technical and trade journals; radio, television, and other mass media; government reports, transcripts of congressional hearings, and publications such as the Congressional Record and the U.S. budget; social media; laboratory publications; and sales and vendor documents.

At the local OPSEC level, facility publications, job ads, solicitations, reading rooms and libraries, and information accessible through electronic information sources such as the internet could represent viable troves for open source exploitation.

3.2.4.6 Computer Intrusion for Collection Operations

It is unclear to what extent foreign intelligence services are using computer hackers to obtain proprietary data or sensitive government information, or whether they have developed the capability to use computer intrusion techniques to disrupt telecommunications activities. Examples of activities include:

In March 2016, an unidentified cyber actor gained access to the network of a US regional water service provider. Exploiting an outdated server, the attacker used a payment application to access the software controlling the flow of chemicals into the water supply. The attacker was able to manipulate the chemicals but was largely a nuisance due to the chemical levels being quickly detected by human operators. Had the attacker possessed greater knowledge of industrial control system applications, the effects could have resulted in a severe threat to public health.

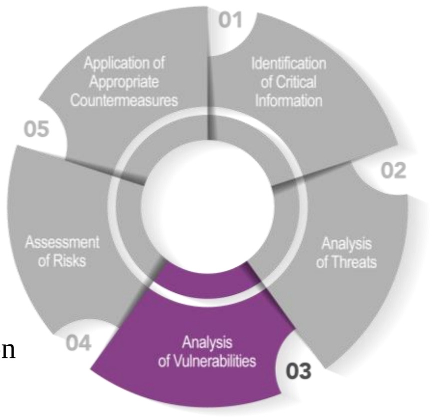
In January 2003, personnel at a U.S. nuclear power plant were unable to access the safety parameter display system due to the Slammer worm. The worm traveled from a consultant's network to the process control network for the power plant. The network traffic generated by the worm inundated the control network, preventing access to the system for 4 hours and 50 minutes.

An article from August 1, 2018, describes how one of the 12 alleged Russian hackers indicted for the Democratic National Committee hacks attempted to use social engineering to get exploits. Ivan Yermakov, a Russian intelligence officer, is alleged to have used the alias Kate S. Milton. While operating under this alias, Yermakov reached out to an unnamed Russian-speaking cybersecurity researcher offering to share malware samples and help with analysis in exchange for access to any exploits she may have. The researcher, who runs a malware-sharing site in addition to being a professional security engineer, suspected that "Milton" was not who she said she was, and later her suspicions were confirmed by the FBI indictment. She turned her communications with Yermakov over to authorities. Chat logs between the two detailed their interactions, culminating in Yermakov offering to buy an exploit for a new vulnerability affecting Microsoft Windows. The researcher declined to make any sale and that was the last she heard from “Milton.”

Analysis of the threat is the second step in the OPSEC process. National-level threat assessments and the DOE design basis threat provide a foundation for the development of the local threat statement. Be imaginative in your thinking to ensure all threats are considered. Remember, the purpose of the threat statement is not to determine if the capabilities of the adversary place your facility or site at risk (assessments perform that function), but simply to identify threats.

3.3 Step 3 – Analysis of Vulnerabilities

OPSEC employs many tools to protect classified and unclassified information of a sensitive nature which may also be controlled unclassified information, but no tool is more important than the OA, as this is the backbone of an operationally effective OPSEC program. An OA is the analysis of an organization, activity, or exercise to identify sources of information potentially exploitable by an adversary, and development of recommendations to mitigate these vulnerabilities. OAs may be broad-based assessments that use the “facility” approach and involve nearly all facets of the organization or facility, or they may be narrower in scope, focusing on a single program or exercise, using the “programmatic” approach.


01
Identification of Critical Information
02
Analysis of Threats
03
Analysis of Vulnerabilities
04
Assessment of Risks
05
Application of Appropriate Countermeasures

An OA is a fact-finding not fault-finding process. It is not a security survey, audit, or inspection, but focuses on procedural or systemic issues rather than individual shortcomings. OAs should not be confused with vulnerability assessments (VAs). VAs are a systematic evaluation process in which qualitative and/or quantitative techniques are applied to identify vulnerabilities and arrive at an effectiveness level for an S&S system to protect specific assets from specific adversaries and their acts. VAs are conducted in accordance with DOE O 470.4B, Chg 2, *Safeguards and Security Program*, and DOE O 470.3C, *Design Basis Threat*. Before an OA is considered, check with local S&S and VA personnel to leverage recent threat assessments (e.g., hazards analysis, security risk assessments, VAs) that have recently been completed and accepted by the ODFSA.

3.3.1 OPSEC Assessments

An OPSEC assessment is a thorough examination of an operation or activity to determine if there is adequate protection against an adversary. In basic terms, an OA is a methodology to identify "what we do" and "how we do it" from the perspective of an adversary and whether it is sufficient to protect sensitive information from an enemy. Assessments are fact-finding actions meant to identify information sources potentially exploitable by an adversary. Their primary purpose is to support management by identifying and offering mitigating approaches to preclude potential losses of sensitive or classified information.

OPSEC assessments must be conducted at a frequency not to exceed 36 months at facilities that possess Category I special nuclear material (or credible roll up to a Category I quantity), Top Secret, or Special Access Program information within their boundaries.

As with most OPSEC activities, the principles are applied during OAs and can be dependent on activities present. OPSEC assumes the traditional "adversarial" perspective during OAs when evaluating operations. In most cases, OAs are unannounced (or with limited advanced warning) to better determine an organization's true OPSEC posture. This ensures results are more realistic and improves the relevance of management countermeasure decisions. However, OAs can also be conducted announced with applicable staff and management acting as trusted agents. Each approach has its pros and cons.

Although the phases below are presented as separate and distinct activities, in practice, some typically overlap. The phases are applicable whether conducting a broad-based, facility-wide assessment or assessing a single narrow function. The breadth and depth of actions related to each phase may be modified as necessary.

OPSEC indicators are the collectible or observable clues that can lead an adversary to critical information and can be discovered in planning or when conducting reviews and OAs.

3.3.1.1 Assessment Determinations

An assessment determination identifies the where, what, and how of the assessment. The first decision is to determine where the assessment will be conducted. The next decision is to determine the approach to be used. The approach begins to identify the "what" and "how" of the assessment.

3.3.1.2 Approach

Both the facility and programmatic approaches have advantages and disadvantages.

Facility

In most instances, identifying a facility is straightforward; it is simply a building wherein a specific program or programs are accomplished in their entirety. For some sites it may not be so easy. A facility may be within a fenced complex containing many buildings and structures, and a program may cross building boundaries throughout the complex or even beyond. In such instances, it may be prudent to conduct programmatic assessments rather than a facility assessment.

In the facility approach, all programs at or within the facility are included in the assessment. The facility approach involves a broad spectrum of both technical and support activities throughout the organization. Conventionally, the former may include weapons programs, research and development activities, production operations, or other missions such as testing, waste management, or cleanup. Support activities include administrative and logistical functions such as personnel services, procurement, computer operations, waste disposal, budget, shipping/receiving, visitor control, protective force operations, etc. Under the facility approach, the critical information list is used to focus the assessment effort. While it is not necessary to address every item listed, efforts should be directed toward items of highest priority.

The facility approach can be time- and manpower-intensive and, depending on the size of the facility, data gathering can be overwhelming. The entire OA team is normally required when using the facility approach. Due to these considerations, it may not be practical to attempt a facility assessment for large facilities.

Programmatic

The programmatic approach focuses on all activities within a single program. If this approach is selected, the organization, activity, program, or technology must be identified. These could include a specific weapons program, a research and development program or project, an exercise, the movement of sensitive material, or any of the vital activities performed at a facility. However, the activity must have a relationship to critical information deemed to require protection from adversary exploitation. In other words, it must have a direct connection with, and should normally be included on, the critical information list. As in the facility approach, activities that provide support to the program may also be assessed. However, only actions directly related to the subject program or project should be included and, contingent upon resource availability, it may be necessary to limit that effort to activities and actions of highest priority. Although there are exceptions, the programmatic approach is not as time and/or manpower intensive as the facility approach.

3.3.1.3 Methodology

The assessment methodology continues to identify the “what” and “how” of the assessment. The methodology can either be visible or invisible.

Invisible

The invisible assessment looks at the facility or program from the outside in. This means that the assessor or team is not “read into” the program or critical information list. The OA assessor or team takes a true adversary approach and attempts to gather information on the program or activity much like an adversary would. The goal of the OA is to identify the program(s) and critical information. When conducting an invisible assessment, the team should understand that an adversary will have much more time to collect and analyze information whereas the OA time is limited. Open source information searches and observations play an important role in the invisible assessment. The invisible methodology is not a covert or clandestine activity, but it does take on a more realistic approach from the perspective of the adversary. Site or program managers are always made aware of invisible OA activities while general site population is not.

Visible

The visible assessment looks at the facility or program from the inside out. It is visible because the presence of the assessment team is readily apparent to the facility or program personnel. The OA assessor(s) or team is briefed on the critical information and indicators, and all site personnel are aware of the OA activity. In the visible methodology, the assessment will include interviews with facility or program personnel.

3.3.1.4 Scope and Objectives

The scope completes the “how” and “what” and can be either full or limited.

Full

A full-scope assessment examines all the elements of critical information and indicators. The assessment is more time consuming than a limited or focused assessment. Since all indicators are assessed, the full-scope assessment will meet the requirements of the programmatic or facility assessment.

Limited

There may be times when resources are not available for conducting a full-scope assessment. A limited-scope assessment examines one or more (but not all) elements of a critical information list item(s) and/or indicators. The advantage is that it is not as time consuming as a full scope and only selected team members whose expertise is relevant need to be involved. The disadvantage is that several limited-scope assessments will be necessary until all list items and/or indicators have been assessed.

3.3.1.5 Team Selection and Support

An assessment team is formed when the OA lead, in coordination with the OPSEC federal oversight, selects a candidate facility or activity for an assessment. The team leader determines team composition. The approach, methodology, and scope determine who and what skills are required for the functional areas to be assessed. Team members may be selected based on their technical knowledge (e.g., computer technician, weapons designer, engineer, or communications expert), organizational functions (operations, finance, contracts, budget, etc.), or recruited from outside of the organization, such as personnel from other government agencies, other DOE sites, or external working group members. The OA team may range in size depending on the complexity of the function being reviewed and scope of the OA.

Team members should have a demonstrated capability to exercise sound judgment, have a practical curiosity, be unbiased, and be able to work with others. Team members should also have a good understanding of the nature, purpose, and conduct of OAs.

3.3.1.6 Program and Support Coordination

Coordination requirements may include, but are not limited to:

- Arranging travel schedules
- Identifying and transferring special access authorizations
- Coordinating in-brief date, time, location, and attendees
- Establishing work spaces at the site of the assessment
- Identifying special equipment needs
- Securing administrative support

3.3.1.7 Conduct

The assessment process provides suggested guidance to help the OPSEC manager or practitioner to become familiar with the flow and format when conducting an OA. An OA may consist of one or more of nine phases. These phases need to be flexible and are subject to change depending on the situation.

3.3.2 Phase 1 – Planning and Preparation

Pre-assessment planning and preparation are vitally important as they set the tone of the entire assessment. The preparation phase identifies who, what, when, where, and how the assessment will be conducted:

- **Assessment determinations** consist of identifying the facility or function to be assessed, approach (facility or programmatic), methodology (visible or invisible), and scope (full or limited).
- **Team assignments** are identified by the OA team leader prior to the first team meeting, along with a schedule for both preliminary data collection and onsite date collection phases. The team members should have skills consistent with the facility being assessed. These skills may cover such areas as operations, communications, logistics, or specific scientific and technical disciplines. As a whole, the team should have an understanding of the activity being examined, but not be so familiar as to jeopardize an objective analysis. Team members must be appropriately cleared for the assignment. The onsite data collection phase will include, but will not be limited to, interviews, field observations, records review, and analysis. All team members providing input should be instructed that an authorized derivative classifier (DC) or reviewing official (RO) must review all information and ensure that it is properly and appropriately marked. In some cases, as the assessment progresses the team leader may need to adjust assignments and scheduling.
- **Preliminary data collection** should begin as soon as team assignments are made and be completed prior to arrival at the facility. Key individuals involved in planning data collection should begin organizing threat data and open source information as early as possible. Because adversary analysis of the subject facility or program will most likely be carried out against the background of large amounts of open source material, preliminary data collection should also attempt to determine what information on sensitive operations is already in the public domain. When collated and analyzed, open source information often provides a disturbingly detailed picture of sensitive activities. In the event that

critical technologies or other sensitive information are identified, SMEs at the facility should be asked to review the open source information as part of the onsite data collection phase.

Key planners should review their threat statement and coordinate with their intelligence contacts, as appropriate. Contingent on the subject being assessed, DOE headquarters may be requested to initiate a review of national intelligence threat data related to the activity involved. This analysis will allow the OA planners to develop an appreciation of how the activity may fit into an adversary's intelligence collection plan.

3.3.3 Phase 2 – Team Orientation

The orientation is designed to familiarize the team with the facility. It actually begins during preparation and continues to the close of the assessment. The team should follow the same paths of interest as would any hostile intelligence organization. Working with program personnel, the team should attempt to gain an understanding of the activity in a brief period. The key to success is cooperation and learning the details of the activity or facility. To obtain an ideal analysis, the route taken must be a fact-finding expedition, not a fault-finding exercise.

3.3.4 Phase 3 – Introductory Briefing

Normally held on the first day of the assessment, introductory briefings are generally conducted at the facility where the assessment is to take place and are conducted by the OA team lead and key facility personnel. This is as much an information exchange between the OA team and facility personnel as it is an overview. The team leader should introduce the members of the team and brief the attendees on the overall OPSEC process and how the OA will assist the facility or program manager in protecting information. The team explains how they will perform the assessment, the scope, what they will examine, and how the assessment will be used. Facility personnel will be asked for recommendations and details on the areas of evaluation and conduct of operations. Depending on circumstances, the introductory briefing may be waived or handled telephonically.

In many instances, this is an opportunity to promote better understanding of OPSEC by conducting a short awareness briefing. It is also important to emphasize that this is not an inspection. It should be made clear that if reportable violations are discovered, the team leader has the responsibility for reporting them through the appropriate channels.

3.3.5 Phase 4 – Field Data Collection

Data collection plans cover the primary areas of OPSEC concern and aid in maintaining the team's focus. Field data collection should include, but is not limited to, interviews with operations and support personnel at all levels of the organization, direct observation of as many operational functions as practical, records and information reviews, and careful examination of all information channels associated with the operations. Some activities and systems that crosscut almost all facilities and programs are described as follows.

3.3.5.1 Open Source Material

Open source material is the large amount of unclassified information usually available to the public, including websites, social media, published articles, news releases, unclassified internal documents, etc. The OA team needs to identify what program- or facility-specific information is available to the public. Oftentimes searching for open source materials is like looking for a needle in a haystack. The assessor must be able to focus the search by identifying key words or phrases associated with a facility or sensitive program. During the preliminary data collection phase, it was noted that any adversary analysis of a DOE facility will certainly be carried out against the background of large amounts of open source material and the purpose of the preliminary data collection is an attempt to determine what information on sensitive operations is already in the public domain. During the field data collection phase, it is important to identify the sensitivity of additional information collected. Types of additional open source material that should be assessed include media reporting, publicly released documents, technical reports presented at conferences and other public meetings, and patents.

Internet

One of the greatest indicators of DOE programs, practices, intentions, and procedures is the internet. The proliferation of use for email, social media, marketing, and other information exchanges is explosive. The highly vulnerable internet has become a vast treasure chest of free information for commercial, political, and military adversaries of the United States, activists, terrorists, and criminals. The threat to information placed on the internet is stated repeatedly and constantly in both the commercial and government arenas. Hardly a day goes by when newspapers or other news media do not have a story about some great hacker success, or some theft or fraud committed by individuals abusing the internet.

Radio and Telecommunications

Radio and telecommunications may be assessed based on inherent vulnerability to monitoring. Many DOE facilities depend heavily on radio communications and virtually all facilities depend on telecommunications. Vast amounts of data and information are exchanged on these systems. In an effort to understand what equipment is used at the site, where it is located, how it is used, and known vulnerabilities, the OA team should attempt to diagram the system in cooperation with the chief information office. The OA should, in cooperation with the Chief Information Office, identify the equipment in use; assess susceptibility to intercept; and identify particularly vulnerable nodes. Radio communications may range from a few handheld units to multiple nets with repeaters covering hundreds of square miles and uniting outlying sites. The first step in data collection for radio communications is to obtain a comprehensive listing of the nets and their frequencies showing:

- Users
- Sensitivity of traffic
- Types of equipment employed
- Function
- Periods of operation
- Use of repeaters
- Power levels
- Any unique features (e.g., telephone patch)

Consider whether or not an adversary could correlate transmissions with some observable activity going on at the facility. It is also useful to conduct hearing ability tests to obtain some estimate of the distance the transmissions can be heard from the facility.

It is essential to determine if transmission security equipment is available and whether or not it is used on a regular basis. If a limited number of secure systems are available, determine if they are allocated to the highest priority nets.

Telecommunications data collection involves the same process used for radio communications, but can be more complicated. For example, most facilities do not control telephone switching and may not be aware of how their circuits are routed. In some instances, the local telephone company may not be aware of routing outside the local area; therefore, the seemingly simple task of developing a system diagram can be a major challenge and should be done with other offices, such as chief information office, technical surveillance countermeasures, intelligence, counterintelligence, etc. Those diagrams should show:

- Routing of calls within the facility, including location and identification of key equipment, routing of main cable runs, and use of any internal microwave links. Determine if internal calls (from one location to another within the facility) go to an outside switchboard.
- Routing of lines between the facility and the local telephone central. If the switchboard is on the facility, determine if outside calls go through an operator or if anyone can dial directly to an extension.
- Routing of commercial long-distance calls, at least to the point they are mixed with large volumes of other traffic. Identify the carriers and whether they use dedicated circuits, either totally dedicated (the same specific channel always reserved for DOE use) or partially dedicated (a certain number of channels always available for DOE, but not necessarily the same channels). Also, note any special lines or direct voice or data lines to other facilities.
- The presence of any other phone circuits within the facility, such as an emergency operations phone system, a teleconferencing system, or an intercom system. If these exist, how do they operate? Could they be operated in reverse as an eavesdropping net? Do they connect with the standard circuit?
- It is important to identify if anyone has a redial phone and if so, who may deal with customers whose relationship is on a need-to-know basis. Redial phones show the last number dialed. If that number is for a sensitive customer or SPP, the user should be aware to dial another number after talking to a sensitive customer.
- Connections to any outlying stations.
- Any use of mobile stations, cordless phones, or cellular phones.
- Any connections (patches) with radio nets, including paging nets.

While it is important to understand there are different locations, operations and challenges for telecommunications using the internet, for specific information regarding cloud-based environments such as Voice over Internet Protocol (VoIP), contact the Chief Information Office.

Global Positioning System Devices. The rapidly evolving market of devices, applications, and services with geolocation capabilities (e.g., fitness trackers, smartphones, tablets, smartwatches, and related software applications) presents significant risk to personnel both on and off duty. These geolocation capabilities can expose personal information, locations, routines, and numbers of personnel, and potentially create unintended security consequences and increased risk to the mission.

Cellular Telephones. After identifying and diagramming the circuits, assess the system and identify any links that are particularly vulnerable. Personnel using those circuits should be aware of their heightened vulnerability and the circuits should be examined in cooperation with the chief information office to identify means of improvement. Cell phone users think of the instrument in the same manner they think of the desk telephone. The instrument is thought to be ON when in use and OFF when not in use. A cell phone, however, maintains some sort of communication with its cellular service provider unless the unit is turned OFF. Even then some instruments can be activated (turned ON) remotely without the user's knowledge. Since cell phones are wireless and can be carried from office to office or building to building, the potential exists for the inadvertent broadcast of conversations. Policies regarding the introduction of cell phones into the work area, particularly in areas where classified or sensitive unclassified information is processed, should be examined. Adherence to these policies should also be observed.

Voicemail. With today's technology, voicemail may also provide vulnerabilities to interception. What is the software used for voicemail and does the vendor maintain a master password? Master passwords are often used by the vendor to access the system remotely, thereby eliminating onsite repair. Unfortunately, accessing the system also permits the vendor access to user accounts.

Facsimile. Fax machines may be a particular problem because of the technical data they process. Identify where such machines are located, who or what offices use them, and what sort of traffic is passed over them.

Secure Telecommunication Devices. Determine if secure telecommunication devices are available, such as STE, Viper, satellite, cell or other encrypted communication devices. Be aware of storage and functionality of these devices. For example, are they situated where people who should use them have ready access? Do telephones in sensitive areas have disconnect switches? Are they used? Attempt to identify what routine coordination is accomplished on telephones located in sensitive areas. For specific information work with the Chief Information Office.

Overall, the most pressing question is: Could an outsider easily monitor sensitive traffic on a systematic basis? Specific countermeasures must be considered where the combination of sensitivity and vulnerability is high. This may include encrypting traffic or using alternate transmission means, such as sending a computer file by mail on a thumb drive rather than over a vulnerable data link.

Computers and Computer Networks

Computers and computer networks pose unique OPSEC concerns related to information control. They contain vast amounts of easily accessed, neatly ordered data that is vulnerable to tampering. Enforcing need-to-know is difficult since access is generally to an entire category of data. A disgruntled insider or individual who gains unauthorized access can severely disrupt an operation. Standard computer security practices may be assessed and computing resources reviewed using one or more available techniques, however it is important to understand there are different locations and configurations for data storage. For specific information regarding internet and cloud-based environments, contact the Chief Information Office.

OPSEC personnel should work closely with computer security personnel. They have mutual interests in information control. In most instances, however, computer security assets focus on hardware and software vulnerabilities, while OPSEC personnel focus on available data concerning operations. This data is made available by operations personnel and may provide indicators of sensitive activities. Therefore, computer systems must be assessed to determine potential operational vulnerabilities.

Obtaining a description of the system is a first step in collecting data about it, but it can also be an important step for an outsider trying to get into the system or identify its most critical elements. Determine if layouts of either classified or unclassified systems are readily available to an adversary. Purchase orders or service contracts may describe system equipment in detail and identify modifications. Such information should be protected from routine access by unauthorized personnel. Most facilities have a long-range computer plan, which should be reviewed to determine its usefulness and availability to adversaries.

Knowledge of the software used with an operating system and of the communications network supporting the system could aid intruders. Determine who develops applications programs, and by whom and how software and hardware maintenance is performed.

Information on the physical layout should also be protected. An adversary seeking to disrupt operations may be very interested in the exact location of key equipment or the exact routing of cables.

Classified Computers. Classified computer systems may have OPSEC concerns that are outside the realm of conventional computer security. Connections, for example, may show sensitive associations. For example, adding an encrypted link—perfectly secure from a computer security point of view—could indicate startup of a new program. Ideally, a classified system has no unclassified links and no unclassified output. However, classified systems might produce unclassified reports or input to such reports. If this is the case, determine who designs the reports, who reviews them, and whether or not the process could be manipulated to obtain classified information.

Unclassified Computers. Most facilities have systems with numerous unclassified computer files. Many, such as personnel files, accounting files, and purchasing files, are quite sensitive. Typically, they are compartmented and protected by passwords. But the compartments or the number of users may be so large that there is little actual protection. Ideally, passwords should be randomly generated, carefully protected, and regularly changed. Sophisticated network programs may link many individual databases into a complex interactive system with widespread dial-up access. That is good for operations, but bad for OPSEC.

Protection accorded each computer system should be assessed to determine if it is adequate for the sensitivity of the data it contains and of the data contained in any other system with which it networks. It may be appropriate to encrypt some lines, ensure that certain transmissions take place over specified circuits, or replace some transmissions with courier or mail service. The objective is to find the optimum balance between security on the one hand; and cost, timeliness, reliability, and common sense on the other.

Controlling computer access is of little value if the output is printed on paper and distributed throughout the facility and elsewhere. The distribution of such products and their ultimate disposition should be determined. Excellent computer security can be defeated by poor control of the products of the system.

It is important to keep in mind that computers are no longer a world unto themselves. Numerically controlled machines, fitness monitors, hi-tech watches, gaming systems, industrial robots, drones, and artificial intelligence systems are a few examples of systems that have their own embedded computers and that may interface directly with computer networks. The OPSEC professional has to keep all of these in mind (along with emerging technologies) as they implement their plan.

Trash

Trash, recycling, salvage yards, and similar services are assessed and analyzed because of the potential for sensitive data to enter these pathways.

Trash invariably contains such matter as scraps of notes and other written materials, discarded wrappers, and shop sweepings. OPSEC personnel should know where trash is accumulated, how accessible it is to outsiders, who collects it, and what the collectors do with it. Contracts should obligate the contractor to destroy the material consistent with the requirements contained in the DOE Orders and locally approved site procedures and OPSEC personnel should verify compliance by unannounced spot checks to validate that the material is being properly destroyed. At a minimum, local site procedures would require the contractor to destroy the material or deliver it to a well-run landfill, and OPSEC personnel should verify compliance by unannounced spot checks to validate that the material is being properly destroyed or left undisturbed.

The concerns about general trash are magnified in regard to paper waste. The first step is to determine how the system works. How is paper waste collected, where does it ultimately end up, and how accessible would it be to systematic collection or occasional screening by an interested outsider? Ideally, trash and paper collection points are on a closed facility; outsiders do not have access to dumpsters or other containers; facility personnel collect the material on a regular basis; the material is brought to a sanitary fill on the facility where it is promptly covered by dirt; outsiders are not allowed access to the sanitary landfill; and operating personnel are alert to any signs of digging or scavenging.

It is one thing to describe how a system should work and another to determine how it does work. Enough information should be gathered to determine how the system really functions. For instance, does a weekend or a late evening visit to the normally neatly covered landfill reveal papers and other material blowing around in the breeze?

Recycling programs are often economically sound, but can be particularly worrisome from an OPSEC viewpoint. If they are not controlled, these programs could assist an adversary's collection activities. By systematically destroying large amounts of sensitive material, a recycling program can perform a welcome OPSEC service. Ideally, the ultimate receiver should be contractually obligated to destroy the material locally and in a controlled facility.

Dumpsters or trash collection points that are accessible to outsiders should be randomly checked. “Dumpster diving” entails rummaging through the trash, collecting a representative sample of papers or other materials of interest, and systematically reviewing them to determine their sensitivity. Consider things such as:

- Is anything classified or sensitive?
- What could someone learn from these materials?
- What procedures are involved in handling the trash and what is its ultimate disposition?
- What physical protection is provided?

Practical measures to reduce vulnerabilities include:

- Shredding, burning, or otherwise destroying sensitive papers before they enter the waste stream.
- Requiring the use of a landfill on the facility.
- Reducing access at critical points in the operation (e.g., locking dumpsters).
- Developing stricter control procedures and a monitoring program to ensure compliance.

Salvage

Salvage materials include serviceable equipment no longer needed, unserviceable items, surplus equipment, and machine turnings sold as scrap. The OPSEC challenge is to ensure they do not provide sensitive information or indicators to unauthorized individuals. In reviewing salvage, check both the paperwork and the items themselves. Consider such things as:

- Do records at the salvage point show what program or account released the material for sale?
- Does the buyer receive such information?
- Is material from sensitive activities systematically inspected before it is turned in for salvage?
- Does the material itself reveal anything of value to an adversary, such as size or shape of a product or simply the fact the material is being used at the facility?

Reports

Program-related information such as reports, internal and external documents, patents, scientific publications, facilities engineering, budget data, and procurement information could present concerns for an OPSEC program. Countless reports are generated within and between DOE facilities, contractors, and other agencies or activities. Many if not most of these reports are unclassified. The reports are both technical and administrative, and represent a collection of data related to DOE programs, activities, and facilities. Because of the constant demand for information, reports flowing up through the levels of management often provide excessive detail and are subject to broad dissemination.

The assessment team should review reports and the reporting system. The review should identify and describe the overall reporting system at the facility; specifically:

- Who prepares the reports?
- What type of information is included?
- What number of copies are produced?
- What is the classification level?
- Who is on distribution?
- What is the ultimate disposition?

Internal Use Documents. Every facility also has unclassified documents prepared for internal use. These documents range from materials, such as newsletters, which may be prepared in multiple copies, to individual notes and memos. Inevitably, much of this material becomes available to the public at large, and much of it is susceptible to a Freedom of Information Act request.

Public Media. Public media runs the gamut from material prepared for the general public to technical publications for special interest groups. Much of what the public media prints about DOE involves information obtained from interviews and tours of facilities, informal discussions with personnel, semi-official visits to operational facilities, and simply local interest stories. This type of writing is often done in conjunction with a DOE public affairs office and can provide glimpses into many sensitive areas, such as names and procedures associated with a specific program. That information could be very important to an adversary trying to develop an understanding of a system or program and its projected activities.

Public Releases. Material in the public media is supplemented by material that the government publishes and releases. In fact, there is no clear line. The voluminous public record is a major source of what is in the public media. Annual reports and transcripts of congressional hearings, for example, are major sources of information on the scope and status of programs.

The conflict between the public's right to know and the government's responsibility to protect sensitive information related to some programs is exemplified by environmental reports, particularly environmental impact statements. Specific legal requirements establish what must be included in an environmental impact statement. Yet, environmental data could reveal sensitive process details. Publicly released data may often contain information beyond that which is required to satisfy the purpose of individual documents. This requires close coordination between OPSEC personnel and those responsible for producing such reports.

Patents and Scientific Papers. Patents and scientific papers often provide details of technical processes at the forefront of developing technology and are therefore described together. Patents and scientific papers often address sensitive details of current processes and are typically indexed in electronic data bases. Additionally, presentations of papers may include much informal discussion, providing a significant opportunity for leakage. This problem requires careful screening of papers and a high degree of security awareness on the part of the person or persons involved. Nevertheless, there are several major difficulties:

- Implications of a technical achievement are not always clear, so information may be released before the full technological impact or the potential classified applications are recognized.
- Classification determinations are often made on the basis of one specific patent or article and its relation to a specific classification guide. Cumulative effects are difficult to address, so sensitive technical information can easily be released piecemeal. This "compilation effect" may dictate that later reports be classified or given an appropriate marking such as Unclassified Controlled Nuclear Information or Official Use Only.

Procurement Cycle. The procurement function represents a viable target for adversary exploitation. This is at least in part due to the fact that it generates voluminous amounts of documentation and it must maintain an audit trail.

The procurement function generally operates in a cyclical mode with five steps:

1. Generating a need, normally submission of a requisition or purchase request from the user.
2. Selecting a supplier, performed by the buyer in the procurement office.
3. Documenting the purchase, formalized by consummating the contract between the purchaser and supplier.
4. Providing the item or service by the supplier.
5. Paying the supplier.

Each step in the procurement cycle generates documentation. OPSEC should determine the degree of accessibility an adversary might have to that documentation and whether or not it provides sensitive information or useful indicators thereof. While practicality demands that most procurement systems operate in an unclassified mode, it must be realized that procurement actions may provide indications or details of very sensitive activities.

The documentation provides numerous elements of information. For example, it identifies many individuals by name and perhaps reveals their job title, office location, phone number, and cost account code. It normally identifies the buyer and seller and includes telephone numbers, addresses, and other similar information related to each. It undoubtedly provides a detailed description of the goods or services being procured and designates a location where delivery is to be made or the service is to be performed.

The potential for correlation of elements of information in the above example is obvious. A given individual located in a specific office or element of the facility has a need for a specified product or service, for use in a designated program or project (identified by the account code). A specific buyer has contracted with a specific supplier whose address is identified to fulfill the need. OPSEC personnel should determine whether or not this type of system is placing sensitive information or activities at risk within the facility or program(s).

Facilities Engineering. Information on the detailed physical layout of a facility can be of great value to an adversary. It could be used in planning and executing an operation against the facility or it may simply add to the adversary's intelligence database. An adversary planning to disrupt operations or obtain material or information must identify the target; know exactly where it is, how to get there, and how well it is protected. Such information could be obtained from engineering drawings or other material produced by engineering organizations.

Publicly available site maps typically provide general information of interest to an adversary; engineering drawings and contract specifications may provide the specific details. They often reflect information on building layouts, process lines, and utility systems. In some instances, they identify the location of vaults, key offices, or sensitive operations. Security features, such as wall thicknesses, fence lines, security posts, and alarm systems, may also be detailed.

Details concerning the accessibility and sensitivity of the information should be obtained.

- How much of it is available in unclassified computer systems?
- Is it passed to contractors to solicit bids or to support activities?
- Are there outside agencies (e.g., a local fire department) who require this information?
- Overall, what information is distributed?
- To whom?
- What controls are placed on it?

Other Data Collection Activities

The following list provides opportunities for an adversary to collect information and should be included in the assessment process:

- Conversations in public places
- Open areas/windows
- Job postings (internal/external)
- Company credit cards
- Travel documentation
- Bulletin board postings
- Foreign national visits/assignments
- Foreign travel reports
- Imaging vulnerability
- Cooperative Research and Development Agreements
- Technology transfer efforts
- Telephone logs
- Employee suggestion programs
- Work for others or SPP
- Janitorial services
- Protective force operations

This list of topical areas is not all inclusive. Each facility and program may be unique, but data collection fundamentals must consider the identified critical information and indicators related to the facility or sensitive program.

Data collection efforts should be flexible, with schedules able to change on short notice. For large teams, daily team meetings should be scheduled to keep everyone abreast of events. The collection process involves scouring through papers, observing operations, and the possibility holding a constant stream of interviews, often with the facility’s busiest people. It is during this stage that the purpose and scope of the assessment might change as a result of the observations.

3.3.6 Phase 5 – Data Analysis

The data analysis phase is not so much a point in time as a gradual transition, with the collection process itself becoming ever more analytical with each passing day. Preliminary drafts of observations and findings are generated to help direct continuing data collection and provide focus during team meetings. The key to the analysis process is doing it from the hostile interest’s point of view. This makes it highly subjective. In effect, the OA team adopts the adversary’s mind set. The OA team attempts to follow the same indicators or pathways the adversary would take to arrive at the critical information. To do otherwise would defeat the purpose of the assessment.

Due to the large amount of data collected during an OA, the team should decide early how to organize it. It could be sorted by functional areas, distinct missions, phases, or program. Sorting the data systematically puts the information into a clear operational perspective, helps keep the data manageable, and makes referencing more convenient during analysis.

As part of the analysis phase when potential vulnerabilities emerge, the vulnerabilities should be validated by the team in conjunction with appropriate facility or program personnel and be classified as appropriate. Particularly, sensitive issues should be brought to the attention of senior facility or program management by the team leader. The team should always maintain the fact-finding not fault-finding philosophy.

3.3.7 Phase 6 – Draft Report

A draft report should be prepared at the conclusion of the assessment. The draft OA report should include, at a minimum, documentation of observations, analysis, and preliminary recommendations.

Observations are any issues or vulnerabilities identified during the assessment, including pathways that adversaries could exploit and an explanation of how they could be used and what information could be revealed. Suggestions are potential countermeasures that a manager or decision maker could implement to protect information that is vulnerable. Since it is the responsibility of the manager or decision maker to review and determine whether or not to implement a suggestion, there should be sufficient information provided to help make an informed decision. The manager or decision maker should be presented with alternatives, if possible, rather than just one solution. The draft report may also document actions taken during the assessment process to mitigate identified vulnerabilities or prevent disclosure of sensitive information. In addition to these topics, it is suggested that assessment reports include the following:

- Purpose of the OA
- Scope of the OA
- Constraints that influenced the results
- Methodology used in collecting data
- Applicable critical information and indicators
- Pertinent threat information
- Acknowledgment of support (accolades)

The draft report and related notes/correspondence should continually be reviewed for classification.

3.3.8 Phase 7 – Exit Briefing

At the conclusion of the assessment, whether visible or invisible, the assessment team should conduct an exit briefing that highlights the results of its effort. This briefing will help explain the observations and information that may be contained in the report and answer questions that may arise. The originator of the report is responsible for ensuring the resulting assessment report is properly reviewed and marked for classification. Senior management, key personnel from the subject activity or facility, and others as appropriate should be invited to attend the briefing. At this time, a copy of the draft assessment report should be provided to the senior manager.

Unlike the introductory briefing, this is a formal briefing covering specific subjects that could include:

- The critical information item(s) and associated indicators as they relate to the activity or facility
- A review of the general and local threat profile
- A synopsis of the team’s observations
- Recommended countermeasures
- Accolades for positive acts noted during the assessment such as maintaining a strong security culture, having a robust OPSEC program, cooperation with the team from staff members, etc.

3.3.9 Phase 8 – Final Report

Providing a draft report to the facility or program manager provides key management and other facility personnel the opportunity to review and comment. (Appendix C provides a sample format for an OA report). However, in some instances additional data and information will be discovered that was not available to the team at the time of the exit briefing.

Before issuing the final report, the facility or program manager should have the opportunity for a final review and comment. Following the review and comment process, the final report should be prepared (do not forget the classification review) and forwarded to the manager through the cognizant DOE federal oversight. Finally, a copy of the OA report and supporting documentation should be retained as a part of the OPSEC program files.

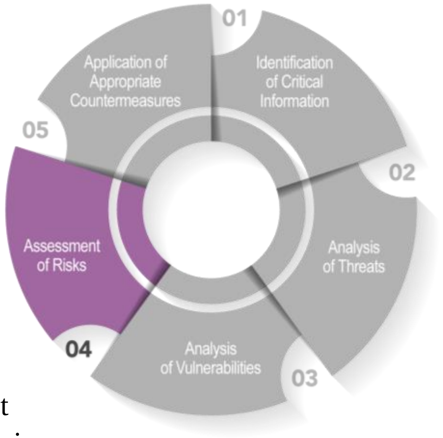
3.3.10 Phase 9 – Follow-on Tasks

Whenever an assessment report includes suggestions, it is important to periodically follow up with the facility or program manager to review actions taken. However, the decision whether or not to implement any suggestion is at the discretion of that manager, for it is the decision maker who accepts the risk.

3.3.11 Summary

The OA process is flexible and adaptable. Although the phased process outlined above is a proven management tool, it may be modified to meet specific requirements. The makeup of the OA team can often be a determining factor in the success or failure of any assessment. Care should be taken to ensure that suggestions accompany any observations made and that the assessment report includes credit in areas where positive action is being taken to protect sensitive information.

3.4 Step 4 – Assessment of Risks


01
Identification of Critical Information
02
Analysis of Threats
03
Analysis of Vulnerabilities
04
Assessment of Risks
05
Application of Appropriate Countermeasures

The assessment of risk is the fourth step of the five-step OPSEC process. Risk assessment is the heart of the OPSEC process. In a risk assessment, threats and vulnerabilities are compared to determine the potential risk posed by adversary intelligence collection activities targeting an activity, program, or organization. When the level of vulnerability is assessed to be high and the adversary threat is evident, then adversary exploitation is expected, and risks are assessed to be high. When the vulnerability is slight, and the adversary's collection ability is rated to be moderate or low, the risk may be determined to be low, and no protective measures may be required. Based on the assessed level of risk, cost/benefit measures can be used to compare potential countermeasures in terms of their effectiveness and cost.

The goal of the OPSEC program is to support the operations of a program, project, facility, activity, event, exercise, etc. Total security can equate to zero operational capability. If everything is totally secure, there is no movement, no access, and no use of the asset. Therefore, total security means no production or results. Since we cannot operate in such an environment, we must accept a certain degree of risk. OPSEC supports the operational decision maker in determining the level of risk that is acceptable.

3.4.1 NSDD 298

NSDD 298 clearly states the responsibility for the level of OPSEC application lies with the activity owner or decision maker. When deciding the degree of OPSEC application, the manager or decision maker must consider the impact of loss associated with the asset, how much risk can be accepted, and how much he or she is willing to spend to reach an acceptable level of risk. DOE O 470.3C, *Design Basis Threat* and DOE O 470.4B state the acceptance of risk is the responsibility of a Federal employee. High risk to certain DOE assets have to be accepted by the Secretary of Energy and moderate risk is accepted by the Program Office.

3.4.2 Risk Determination

The risk assessment phase provides the decision maker with a firm foundation upon which to make a risk management decision. Information necessary to the decision-making process relates directly back to the first three steps of the OPSEC process: identify critical information, analyze the threat, and analyze vulnerabilities. Critical analysis provides decision makers with information concerning their assets and how vulnerable those assets are to threatening acts. As a function of risk analysis, management must always be aware of the bottom line—how much will recommended countermeasures cost? With this information they will weigh the impact of the loss or compromise against the countermeasure.

Risk analysis helps determine whether the adversary has the intent and capability to exploit vulnerabilities and, if so, the potential impacts. Risk can never be completely eliminated, which is why we must have a system to manage and reduce the risks to our critical information/operations.

$$\text{Threat} \times \text{Vulnerability} \times \text{Impact} = \text{Risk}$$

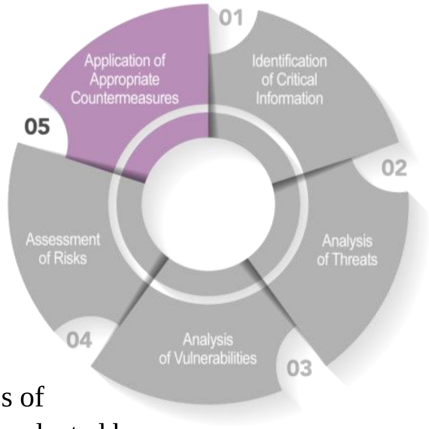
Threat is the adversary's intent and capability, **vulnerability** is the weakness that provides the adversary's opportunity, and **impact** is the potential negative consequences inflicted upon a programmatic mission or facility. Risk assessment helps a decision maker identify which vulnerabilities require protection and the amount of protection of countermeasures that are to be applied. The level of risk associated with each vulnerability will help prioritize the application of resources. It is important that all personnel use the same scale when assessing the vulnerabilities and threats. What is the cost if the threat exploits the vulnerability? The cost is not just money. “Cost” must also take into account:

- People – what is the potential loss of life or severe injury?
- Time – what happens if the operation/mission does not happen on time?
- Money – what will it cost to secure?
- Resources – what other physical resources are at risk: weapons, computers, vehicles?
- Reputation – what are the public and professional perceptions?

Risk analysis answers these questions:

- How likely is an adversary to exploit a particular vulnerability?
- What are the consequences if it does?

3.5 Step 5 - Application of Countermeasures


01
Identification of Critical Information
02
Analysis of Threats
03
Analysis of Vulnerabilities
04
Assessment of Risks
05
Application of Appropriate Countermeasures

The OPSEC Program can assist managers in developing and to a certain extent implementing countermeasures to mitigate vulnerabilities to their programs and activities. In this step, countermeasures are developed that will ideally eliminate the adversary threat, the vulnerabilities that can be exploited by the adversary, or the utility of the information. In assessing countermeasures, the impact of the loss of critical information on organizational effectiveness must be balanced against the cost of implementing corrective measures. Possible countermeasures should include alternatives that may vary in terms of feasibility, cost, and effectiveness. Based on the probability of collection, the cost effectiveness of various alternatives and the criticality of the activity, countermeasures are selected by the program manager or decision maker. In some cases, there may be no effective means to protect information because of cost or other factors that make countermeasure implementation impossible. In such cases, the manager must decide to accept the degradation of effectiveness or cancel the activity. As a reminder, DOE O 470.3C, *Design Basis Threat* and DOE O 470.4B state the acceptance of risk is the responsibility of a Federal employee. High risk to certain DOE assets must be accepted by the Secretary of Energy and moderate risk is accepted by the Program Office (Dash 1).

The process begins with an examination of the totality of an activity to determine what exploitable but unclassified evidence of classified or sensitive activity could be acquired in light of the known collection capabilities of potential adversaries. Such evidence usually derives from openly available 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, they are analyzed against the threat to determine the extent to which they may reveal critical information. The threat and vulnerability analyses are used in risk assessments to assist in the selection and adoption of appropriate countermeasures.

There are hundreds of cost-effective countermeasures that can be used against existing and future vulnerabilities. The OPSEC Program should maintain a generic list of countermeasures that are available for utilization.

The examples included in this section are by no means a complete list of countermeasures. The list is theoretically endless and limited only by imagination and available funding. Again, the primary consideration before implementing OPSEC countermeasures is the threat and cost versus risk considerations.

- Shredding waste material
- Locking offices and file cabinets
- Adopting a "clean desk" policy
- Changing outdoor activity
- Limiting distribution of site information such as organization charts, site phone books, email listings, etc.
- Modifying routines
- Covering material stored outdoors
- Adopting cover stories for sensitive activities
- Using correct radio procedures
- Reviewing publications before they become public
- Maintaining awareness of sensitive information on travel requests
- Guarding telephone conversations and not discussing sensitive information over the telephone
- Encrypting data before transmission
- Paying attention to casual conversations (where and who may be listening)
- Sanitizing conference rooms to include erasing whiteboards at the end of the meeting/end of the day.

Dependent on available resources, the OPSEC program may initiate varying levels of rigor when implementing countermeasures. Examples of varying approaches are included in Table 3.1.

Table 3.1. Three Levels of Rigor in Approaching OPSEC Issues

Issue	Sufficient	Rigorous	Restrictive
Protect emailed information	Send attachment in encrypted email; sanitize subject line.	Send encrypted email with link to Metagroup folder that includes file; sanitize subject line; periodically break email chains.	Send encrypted email with link to Metagroup controlled folder; protect file with password; sanitize subject line.
Conduct vendor assessments	Conduct high-level vendor assessment for all vendors; Conduct deeper vendor-assessment reviews for vendors of critical components.	In addition, provide Counterintelligence with list of selected vendors for review; provide staff training in supply chain risk management.	In addition, review high-level vendor assessments annually, and examine relationship "footprint" (or an indication that such information is available).
Scrutinize publications	Review draft articles, papers, and presentations with team or program lead.	In addition, review draft articles, papers, and presentations with Counterintelligence.	In addition, review draft articles, papers, and presentations with TRUST engineer.

Control physical access	Implement access controls (e.g., badge reader) in areas where components and materials are stored.	Lock components and materials in cabinets when unattended.	Place ordered components and materials in locked containers.
Information storage	Metagroups, access storage.	Controlled (periodically reviewed) metagroups, file passwords.	Restricted-access PRIME storage, controlled (periodically reviewed) SCN metagroups.
True change cannot come from a checklist: INFOSEC issues and mitigations differ across teams and sites.			

In the OPSEC process, it is important to distinguish between analysis of threat and vulnerability on the one hand, and implementation on the other. Recommendations on the use of OPSEC measures are based on joint operational-intelligence analyses, but ultimate decisions on implementation are made by supervisors or program managers who determine the aspects of a program or activity to be protected. The decision maker with ultimate responsibility for mission accomplishment and resource management will have authority for determining where and how OPSEC will be applied. Therefore, their full understanding of the OPSEC process, concerns, and recommended countermeasures is vital. Refer to the DOE O 470.3C *Design Basis Threat* to ensure security risk acceptance determinations are presented to authorized personnel (see also Section 3.0).

4.0 MAINTAIN THE PROGRAM

4.1 Management Updates

One responsibility of the OPSEC manager or practitioner is to provide management with the information required for sound risk management decisions concerning the protection of sensitive information. It is therefore imperative that managers receive regular OPSEC briefings and updates to ensure the intent and status of the program is understood. Activities may appear insignificant when considered alone, but when viewed with other indicators, they may present a risk to the mission or operation.

It is important to obtain the approval and support of senior management once the list of critical information and related indicators are completed. The information supports a number of activities to include when establishing an OA schedule and conducting OPSEC reviews. This information must be accessible to personnel and managers as a tool when determining who should have access to program or project information and what information may be released. It also is a tool to help management understand the risk in terms of the consequences of loss of the information.

Quarterly or annual leadership awareness briefings should provide a status of:

- Funding and staffing requirements to determine adequate budget for
  - training
  - awareness materials
  - OPSEC manager and practitioner(s)
  - working group members
- Interdisciplinary relationships of the program

- Liaison activities
- Program successes
- Implementation issues and lessons learned
- Proposed solutions and conflicting factors.

The OPSEC program should engage leadership in the creation and implementation of solutions based on best practices (of the site and industry) and lessons learned, and closely follow other program and project management practices (see Appendix F for additional information).

4.2 Recordkeeping

As required by national policy and further defined through the applicable National Archives and Records Administration's guidance, a sound, well-documented system is necessary to ensure the appropriate recordkeeping requirements and lifecycle management of DOE records are maintained. See the most current version DOE O 243.1B, *Records Management Program,* for further information.

4.3 Annual Review/Verification of Critical Information Lists

An annual review of the critical information list(s) should be conducted to identify changes to programs, activities, or facilities that may result in the modification of critical information topics. The review should be a documented, limited information gathering activity that, when completed, will inform the scheduling and implementation of OPSEC actions.

The review should include:

New construction planned for a facility that will process or store classified or sensitive matter

New sensitive activities or existing programs incurring significant changes

A sensitive program or activity that has not been the subject of an OPSEC assessment or OPSEC review for the preceding three years.

4.4 OPSEC Awareness

Development and execution of a comprehensive OPSEC awareness program is an integral piece of the overall OPSEC concept. This includes regular briefings to ensure personnel are aware of their responsibilities in support of the protection of sensitive and classified information. These briefings provide local implementation of national and departmental requirements and may be integrated into or provided in conjunction with required security briefings (e.g., new hire, comprehensive or annual refresher briefings).

The local OPSEC program should strive to instill a spirit of OPSEC awareness among the general site population. Ensure that all personnel understand OPSEC principles and that they consider incorporating OPSEC in their areas of operation.

4.4.1 Briefings

When conducting OPSEC awareness briefings in person, it is important to understand your audience. OPSEC professionals often brief a wide range of people at their sites, both federal and contractor personnel, and all levels of the general population from managers to “worker bees.” Whether you are presenting to a small or large group, there are many things you can to do in advance to ensure your presentation achieves the desired response.

To connect with your audience, you need to understand why OPSEC is important to them. What do they expect to learn from the presentation? It is also important to know the level of knowledge they have about security and OPSEC specifically, so you can present the information with the correct tone to keep people interested and engaged. There is nothing more insulting than to present basic information to a highly knowledgeable audience or speak at a level too high for a novice audience.

You should also gauge the mood of the audience. If the audience seems to be in a lighthearted mood, the speaker can use humor to keep interest. If they seem to be serious or the topic is of a serious nature, then the speaker should get right to meat of the talk.

When you know more about your audience and their expectations, you will be able to tailor your talk to make it more interesting. Your audience will be engaged and satisfied, and you will have help to spread your OPSEC message.

4.4.2 Learning Styles

A learning style is an individual’s preferred way of gathering, organizing, and thinking about information. Adult learners are used to being in charge of their lives and deciding what is important to them. They want acknowledgement of past experiences and can bring a great deal to groups discussions. They expect to get something practical from the training that can be used right away.

Traditional learning styles that may be tailored and applied based on the information being taught include:

Visual. Visual learners need to see everything, need visual stimulation and tend to use visual references when they speak. They prefer to see photos and graphics in training materials.

Auditory or aural. Auditory learners need verbal instruction and use hearing references. They prefer step-by-step instruction. Lectures, group discussions, and verbal question and answer activities work well.

Kinesthetic or tactile. Kinesthetic learners are those who prefer hands-on situations and tend to use feeling references in their speech. They have a hard time sitting still for a long period and prefer to be moving and doing things.

Because training and awareness activities are such an important part of an effective OPSEC program, the OPSEC professional should attempt to incorporate elements of the three learning styles to reach all types of participants.

4.4.3 Activities

A talent for creativity is a true asset when discussing OPSEC awareness. There are many ways to communicate and convey the message. OPSEC program staff should use their OWG members or other site personnel to help design and develop new awareness initiatives. The following list identifies some examples of awareness activities:

- Giveaways. Items such as OPSEC puzzles, purple dragon figurines, certificates, pins, coffee mugs, tee shirts, and fortune cookies have been given to employees who provided good ideas or suggestions, identified potential vulnerabilities, or demonstrated good OPSEC practices.
- Publications. Use of the site’s intranet home page are a great way for the OPSEC program to get the word out to the masses. Articles and/or short messages can be easily changed and updated.
- Site monitors. Many DOE sites have television monitors located throughout their facility that broadcast general site information to their population. This is another good way to share short, easy-to-remember OPSEC awareness tips.
- Shred days. Shred events have proven to be an excellent way to bring OPSEC to fellow employees. The events provide an excellent opportunity to raise general security awareness and allow the OPSEC program to interact with site personnel.
- Contests. OPSEC programs have generated interest by hosting contests in the site newspaper/bulletin where clues (indicators) are provided weekly on a fictitious critical program and employees are encouraged to guess the sensitive project. The winner may get their picture in the paper or be given one a prize.

4.4.4 Concerns

Tables 4.1 and 4.2 are examples of how the publishing of information and the things said or felt may impact the OPSEC program. Biases and a workforce culture that does not fully accept threat hinder information protection.

Table 4.1. What information and in what venues should we publish?

Information	Content	Value
Schedule and budget	Priorities, partnerships, timelines for design-and-production activities and new capabilities	Potential subversion points and their supporting operations, as well as identification of windows of opportunity
Staff awards	Rising leadership, key departments, and significant innovations	Potential targets for recruitment or information
Problems/lessons learned	Design, production, or quality problems or delays	Potentially exploitable vulnerabilities or insight to create and hide a vulnerability
Conference/NNSA presentations (OSTI.gov)	Unique or advanced technologies, changes in technologies, and problems solved	Opportunities to make technical “jumps,” innovations that could lead to issues, and DOE preferences and approaches
Partnerships (vendor, suppliers, universities)	Partners who provide DOE with parts, materials, expertise, or technologies	External and less-secure targets for gathering/ targeting cyber and physical information
Social media (individual posts)	Project status, roles in a program, levels of job satisfaction, and technical accomplishments	Near-real-time updates, potentially disgruntled staff (recruitment), and insights (timeline or technical) not available through official sources

Media (lab news, corporate media releases and posts)	Launch of major initiatives, world-class capabilities and innovations, key personnel, locations of work, and technology preferences	Knowledge about state-of-the-art research or facilities, commonalities between weapons, potential targets, component features, and event to attend

Table 4.2. OPSEC Culture

What we do	What we say
Under-assess value	• I only have a small role. • My information isn't classified or critical.
Fall back on habit, convenience, or familiarity	• We've always communicated on the secure network. • It's a commercial-off-the shelf part. • It's a known vendor.
Use short-term thinking	• It's a prototype. • I may not end up using that vendor.
Assume a security culture	• My team doesn't openly associate the component number, component, and weapon—so others won't. • Why would a vendor show other customers my part? • But it's on a DOE network … (why encrypt? It's not vulnerable, is it?) • It is not covered in the classification guide so ○ …it must not be classified. ○ …I guess I don't need to protect it.
Over-value collaboration	• Nothing about this research is classified. • We collaborate with academic and industry partners.
Over-value storage	• It is on my laptop/USB, so it is protected. • The email was only sent within DOE or to a few people so I don't need to encrypt.

4.4.5 Delivering the OPSEC Message

OPSEC professionals should attempt to fully use today's technologies to help spread their message. Be creative when selecting the best platform. Some examples of OPSEC posters are included in Figures 4.1 and 4.2. Additional examples provided by OPSEC programs will be added to OPSEC Resources on DOE Powerpedia found athttps://powerpedia.energy.gov/wiki/Office_of_Security_Policy.

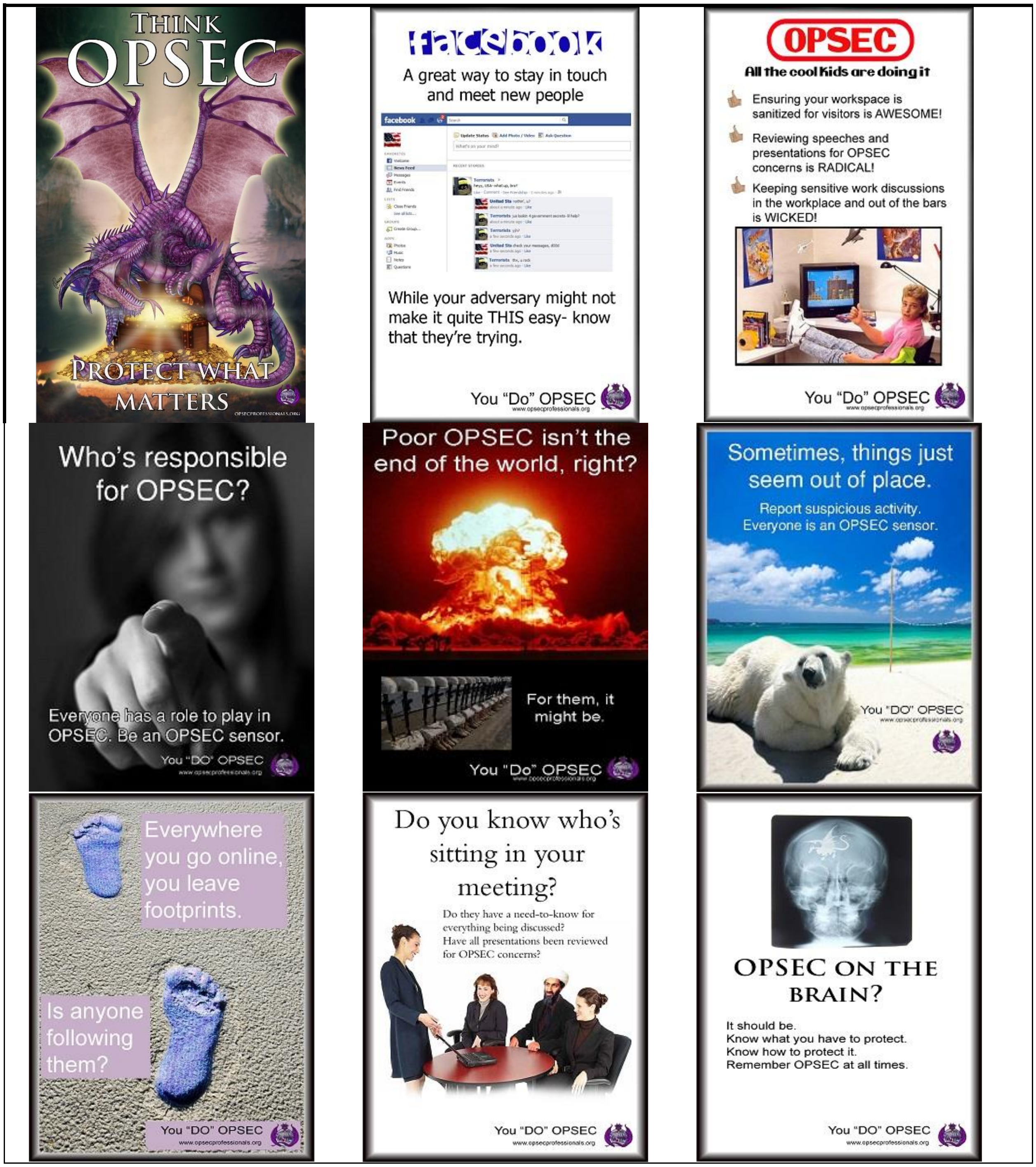

Think OPSEC
Protect what matters
OPSECPROFESSIONALS.ORG
facebook
A great way to stay in touch and meet new people
While your adversary might not make it quite THIS easy- know that they're trying.
You "Do" OPSEC
www.opsecprofessionals.org
OPSEC
All the cool kids are doing it
Ensuring your workspace is sanitized for visitors is AWESOME!
Reviewing speeches and presentations for OPSEC concerns is RADICAL!
Keeping sensitive work discussions in the workplace and out of the bars is WICKED!
You "Do" OPSEC
www.opsecprofessionals.org
Who's responsible for OPSEC?
Everyone has a role to play in OPSEC. Be an OPSEC sensor.
You "DO" OPSEC
www.opsecprofessionals.org
Poor OPSEC isn't the end of the world, right?
For them, it might be.
You "Do" OPSEC
www.opsecprofessionals.org
Sometimes, things just seem out of place.
Report suspicious activity.
Everyone is an OPSEC sensor.
You "DO" OPSEC
www.opsecprofessionals.org
Everywhere you go online, you leave footprints.
Is anyone following them?
You "DO" OPSEC
www.opsecprofessionals.org
Do you know who's sitting in your meeting?
Do they have a need-to-know for everything being discussed?
Have all presentations been reviewed for OPSEC concerns?
You "DO" OPSEC
www.opsecprofessionals.org
OPSEC ON THE BRAIN?
It should be.
Know what you have to protect.
Know how to protect it.
Remember OPSEC at all times.
You "DO" OPSEC
www.opsecprofessionals.org

Figure 4.1. OPSEC Poster Examples

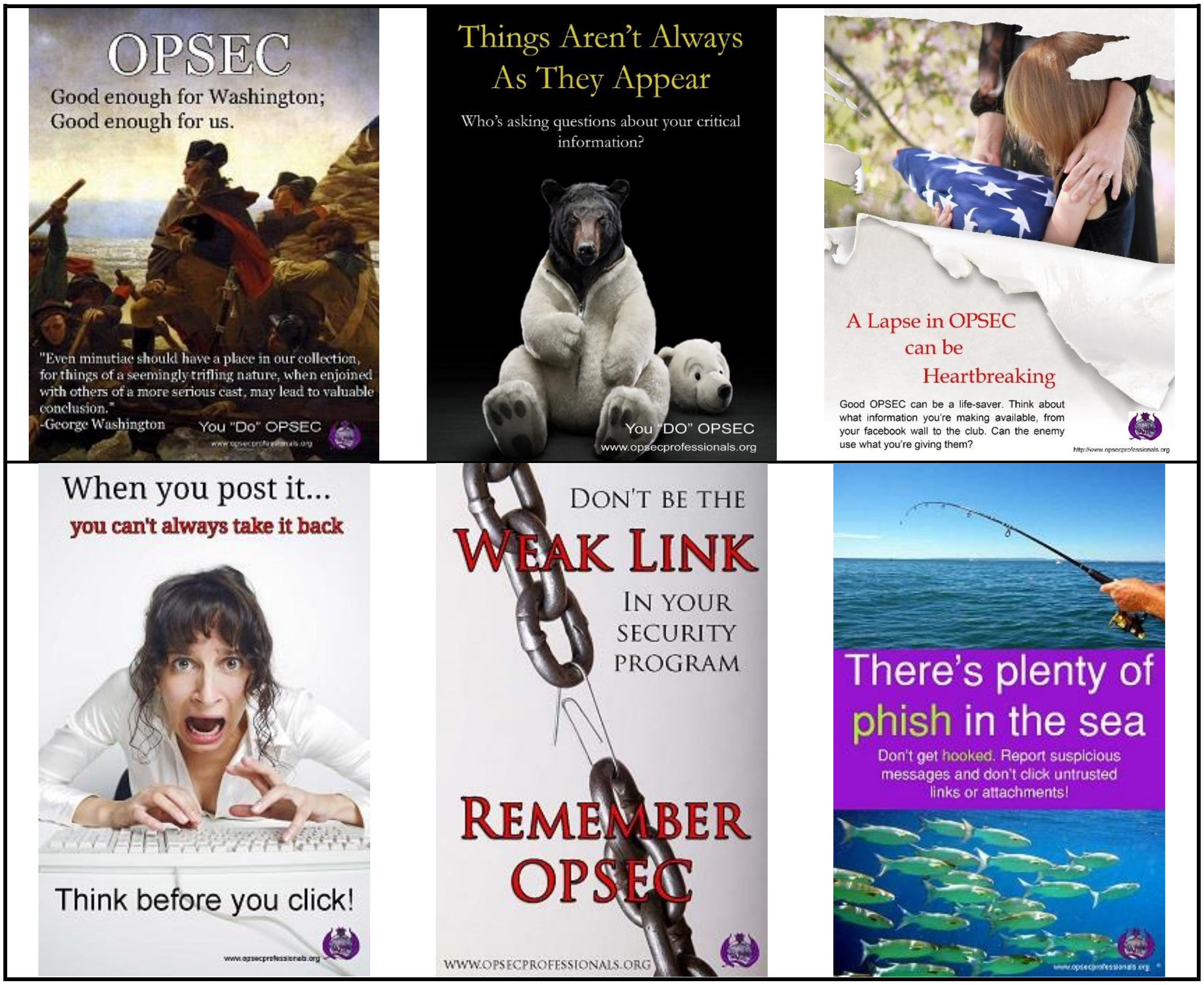

OPSEC
Good enough for Washington;
Good enough for us.
"Even minutiae should have a place in our collection, for things of a seemingly trifling nature, when enjoined with others of a more serious cast, may lead to valuable conclusion."
-George Washington
You "Do" OPSEC
www.opsecprofessionals.org
Things Aren't Always As They Appear
Who's asking questions about your critical information?
You "DO" OPSEC
www.opsecprofessionals.org
A Lapse in OPSEC can be Heartbreaking
Good OPSEC can be a life-saver. Think about what information you're making available, from your facebook wall to the club. Can the enemy use what you're giving them?
http://www.opsecprofessionals.org
When you post it...
you can't always take it back
Think before you click!
www.opsecprofessionals.org
DON'T BE THE
WEAK LINK
IN YOUR SECURITY PROGRAM
REMEMBER OPSEC
WWW.OPSECPROFESSIONALS.ORG
There's plenty of phish in the sea
Don't get hooked. Report suspicious messages and don't click untrusted links or attachments!
www.opsecprofessionals.org

Figure 4.2. Additional OPSEC Poster Examples

Use of computer-based multimedia learning environments—consisting of images, text, and sound—offer a potentially powerful setting for improving understanding. Multimedia content helps to vary and enhance the learning process and leads to better knowledge retention. However, all multimedia resources are not equally effective, so the challenge developers face is how to assess and select multimedia resources that best promote meaningful learning. Although a multitude of information, videos, and training tools is available on the Internet, OPSEC programs should be very careful to adhere to copyright laws and ensure that the open source information is available for use.

4.5 OPSEC Training

It is essential for S&S staff, coordinators, and practitioners receive formal training to function in their roles, build a cadre of trained and knowledgeable practitioners, and maintain an effective OPSEC program. OWG members also benefit from formal training but can receive informal briefings and education from the program or other sources (e.g., OPSEC Professional's Association, OPSEC Professionals Society, and IOSS).

To support OPSEC program training and continuity in keeping to guidance requirements, a list of OPSEC-specific training opportunities has been identified:

- IOSS OPSEC Fundamentals (OPSE-1301) computer-based training or Center for Development of Security Excellence (a Department of Defense organization) *OPSEC Fundamental Course* (IO-OP101.16).
- DOE National Training Center (NTC) eAccess Online Services course ISC-141DE, *Operations Security (OPSEC) Overview*, computer-based training.
- DOE NTC course ISC-241, *Operations Security*, in residence course.
- External OPSEC training courses (e.g., IOSS OPSEC Surveys computer-based training; OPSE-1500, *OPSEC and Public Release Decisions*; OPSE-2380, *OPSEC Analysis*; OPSE-2390, *Program Management*; and OPSE-3500, *OPSEC and Internet-Based Capabilities Course*).
- Various OPSEC professional associations or consultants.

4.6 Summary

As a reminder, this handbook provides general information to assist DOE sites in the development, implementation, and evaluation of the OPSEC program. It is not intended to be an all-inclusive list of activities that must be completed to ensure a compliant program. Rather this handbook is intended to aid in the implementation of a new program, stimulate new ideas for incorporation into an existing program, or provide assistance for problem solving. OPSEC practitioners are encouraged to reach out to others in the DOE community for help or assistance, as needed.

This page intentionally left blank.

Appendix A: National Security Decision Directive Number 298

THE WHITE HOUSE
WASHINGTON
January 22, 1988

NATIONAL SECURITY DECISION
DIRECTIVE NUMBER 298

NATIONAL OPERATIONS SECURITY PROGRAM

OBJECTIVE

Security programs and procedures already exist to protect classified matters. However, information generally available to the public as well as certain detectable activities reveal the existence of, and sometimes details about, classified or sensitive information or undertakings. Such indicators may assist those seeking to neutralize or exploit U.S. Government actions in the area of national security. Application of the operations security (OPSEC) process promotes operational effectiveness by helping prevent the inadvertent compromise of sensitive or classified U.S. Government activities, capabilities, or intentions.

OPSEC PROCESS

The operations security process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate 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 openly available 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, they are analyzed against the threat to determine the extent to which they may reveal critical information. Commanders and managers then use these threat and vulnerability analyses in risk assessments to assist in the selection and adoption of countermeasures.

OPSEC thus is a systematic and proved 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.

APPLICATION

Indicators and vulnerabilities are best identified through detailed OPSEC planning before activities start. They may also be identified during or after the conduct of routine functional activities by analyzing how functions are actually performed and the procedures used. Planning and analysis proceed from the adversary's perspective. To assist in OPSEC planning and analysis, OPSEC planning guidance must be developed jointly by those most familiar with the operational aspects of a particular activity together with their supporting intelligence elements.

OPSEC planning guidance should take account of those aspects of an activity that should be protected in light of U.S. and adversary goals, estimated key adversary questions, probable adversary knowledge, desirable and harmful adversary appreciations, and pertinent intelligence threats. OPSEC planning guidance should also outline OPSEC measures to complement physical, information, personnel, signals, computer, communications, and electronic security measures. OPSEC measures may include, but are not limited to, counterimagery, cover, concealment, and deception.

In the OPSEC process, it is important to distinguish between analysis of threat and vulnerability, on the one hand, and implementation, on the other. Recommendations on the use of OPSEC measures are based on joint operational-intelligence analyses, but ultimate decisions on implementation are made by commanders, supervisors, or program managers who determine the aspects of a program or activity to be protected. The decision maker with ultimate responsibility for mission accomplishment and resource management must have complete authority for determining where and how OPSEC will be applied.

POLICY

A National Operations Security Program is hereby established. Each Executive department and agency assigned or supporting national security missions with classified or sensitive activities shall establish a formal OPSEC program with the following common features:

- Specific assignment of responsibility for OPSEC direction and implementation.
- Specific requirements to plan for and implement OPSEC in anticipation of and, where appropriate, during department or agency activity.
- Direction to use OPSEC analytical techniques to assist in identifying vulnerabilities and to select appropriate OPSEC measures.
- Enactment of measures to ensure that all personnel, commensurate with their positions and security clearances, are aware of hostile intelligence threats and understand the OPSEC process.
- Annual review and evaluation of OPSEC procedures so as to assist the improvement of OPSEC programs.
- Provision for interagency support and cooperation with respect to OPSEC programs.

Agencies with minimal activities that could affect national security need not establish a formal OPSEC program; however, they must cooperate with other departments and agencies to minimize damage to national security when OPSEC problems arise.

ACTION

Heads of Executive departments and agencies assigned or supporting national security missions.

Heads of Executive departments or agencies with national security missions shall:

- Establish organizational OPSEC programs;
- Issue, as appropriate, OPSEC policies, procedures, and planning guidance; and
- Designate departmental and agency planners for OPSEC.

Further, they shall advise the National Security Council (NSC) on OPSEC measures required of other Executive departments and agencies in order to achieve and maintain effective operations or activities. In this connection, the Joint Chiefs of Staff shall advise the NSC of the impact of nonmilitary U.S. policies on the effectiveness of OPSEC measures taken by the Armed Forces, and recommend to the NSC policies to minimize any adverse effects.

Chairman, Senior Interagency Group for Intelligence (SIG-I).

Consistent with previous Directives, the SIG-I has responsibility for national OPSEC policy formulation, resolution of interagency differences, guidance on national-level OPSEC training, technical OPSEC support, and advice to individual Executive departments and agencies. The National Operations Security Advisory Committee (NOAC), as part of the SIG-I structure and functioning under the aegis of the Interagency Group for Countermeasures (Policy), will:

- Advise the SIG-I structure on measures for reducing OPSEC vulnerabilities and propose corrective measures;
- As requested, consult with, and provide advice and recommendations to, the various departments and agencies concerning OPSEC vulnerabilities and corrective measures;
- On an ad hoc basis, chair meetings of representatives of two or more Executive departments or agencies having competing interests or responsibilities with OPSEC implications that may affect national security interests. Analyze the issues and prepare advisory memoranda and recommendations for the competing agencies. In the event NOAC fails to resolve differences, it shall submit the issue, together with its recommendation, to the SIG-I for resolution, which may recommend a meeting of the Policy Review Group (PRG) to consider the issue;
- Bring to the attention of the SIG-I unsolved OPSEC vulnerabilities and deficiencies that may arise within designated programs and activities of the Executive branch; and
- Specify national-level requirements for intelligence and counterintelligence OPSEC support to the SIG-I.

Director, National Security Agency.

The Director, National Security Agency, is designated Executive Agent for interagency OPSEC training. In this capacity, he has responsibility to assist Executive departments and agencies, as needed, to establish OPSEC programs; develop and provide interagency OPSEC training courses; and establish and maintain an Interagency OPSEC Support Staff (IOSS), whose membership shall include, at a minimum, a representative of the Department of Defense, the Department of Energy, the Central Intelligence Agency, the Federal Bureau of Investigation, and the General Services Administration. The IOSS will:

- Carry out interagency, national-level, OPSEC training for executives, program and project managers, and OPSEC specialists;
- Act as consultant to Executive departments and agencies in connection with the establishment of OPSEC programs and OPSEC surveys and analyses; and
- Provide an OPSEC technical staff for the SIG-I.

Nothing in this directive:

- Is intended to infringe on the authorities and responsibilities of the Director of Central Intelligence to protect intelligence sources and methods, nor those of any member of the Intelligence Community as specified in Executive Order No. 12333; or
- Implies an authority on the part of the SIG-I Interagency Group for Countermeasures (Policy) or the NOAC to examine the facilities or operations of any Executive department or agency without the approval of the head of such Executive department or agency.

Appendix B: Sample OPSEC Plan

(NOTE: An OPSEC Plan is often classified. The document should be marked as a final classified or controlled unclassified document with portion markings as required.)

ABC, Inc

OPERATIONS SECURITY PLAN

[Date]

1. PURPOSE. The purpose of this plan is to establish the OPSEC measures required by the Director, ABC for all elements of ABC, Inc. [for what time period?].

1.1. Mission Statement. Protect from loss, damage and compromise the systems, information, data and procedures, as well as the personnel, capital assets and intellectual property, entrusted to ABC, Inc. or created by it that are essential to the successful and responsible achievement of all missions and responsibilities.

1.2. Success Criteria. These criteria are designed to provide a yardstick against which the acceptability of risk can be measured. It is what the Director, ABC, Inc. can realistically expect the ABC, Inc. security, counterintelligence and OPSEC programs to provide, given the vulnerabilities, threats and resources available to counter those threats. The Hazard Consequence Table at Attachment 1 provides a scale by which unacceptable consequences to adversary action, or failures to protect information can be measured. The countermeasures and recommendations described in this plan are designed to achieve risk that will ensure ABC, Inc. assets, people, and missions face no consequences higher than a “medium” intensity. That is:

1.2.1. Injuries; on scene medical treatment or victim(s) transported for minor treatment, and released from hospital.

1.2.2. Delays to an operation of greater than one hour but less than four hours.

1.2.3. Loss of critical information has less than medium impact on ABC, Inc. operations or activities; no loss of classified or SCI information.

1.2.4. Loss of property or financial loss to person(s), ABC, Inc., or the U.S. government of greater than $5,000 but less than $10,000.

1.2.5. Manageable embarrassment or harm to the reputation of ABC, Inc. or the nation.

2. SCOPE AND APPLICATION. The ABC, Inc. Operations Security Plan applies to all functional and operational components under the supervision, management and control of the Director, ABC, Inc.

3. DEFINITIONS. See Attachment X for a glossary of definitions and acronyms.

4. THREAT. Overall, the threat to ABC, Inc. mission, personnel, and assets is [low/medium/high]. ABC, Inc. is now faced with adversaries that have demonstrated both intent and capability to [what are the adversary's intent and capability?]. A detailed analysis of the threat to ABC, Inc. is provided at Attachment X. The following is a summary of this analysis:

4.1.

4.2.

Table 1. Intent and Capability Analysis Summary

	History	Activity	Doctrine	Motivation
Intent				

	Technology	Force Structure	Mobility	Access
Capability				

5. CRITICAL INFORMATION. The following information is identified as critical to the success of the ABC, Inc. mission.

5.1. [Provide critical information list]

6. OPSEC ESTIMATE. The OPSEC estimate is a result of research on what information is generally available in open source, and what the adversary, or adversaries, can reasonably be expected to now know. The estimate also takes into consideration the adversary's intelligence capabilities and demonstrated levels of familiarity with ABC, Inc. based on actions taken against ABC, Inc. or the nation to date.

6.1. The OPSEC estimate provides a baseline of what information has already been made available in open source, or what the adversary can reasonably be expected to know from other sources. For the purpose of this plan, the adversary is defined as [identify adversary here].

6.2. Although not freely available, it should be noted that an employee's ABC, Inc. association is easily obtained through credit records, property records, and other Internet services for a minimal fee. It is very likely that increased scrutiny at border crossings, etc. will be given U.S. citizens in certain countries, significantly increasing the risk to ABC, Inc. personnel in travel status.

6.3. Open source research for this plan was conducted by {name of each member of the OPSEC survey team]; references to corroborate conclusions are kept on file. This list is not all-inclusive. It will expand with further research. The following is a summary of what was found in a cursory review.

7. VULNERABILITIES, RISK, COUNTERMEASURES, AND RESIDUAL RISK.

The following vulnerabilities apply to ABC, Inc. and [Operation/Activity], and the associated risks have been determined unacceptable. Countermeasures will be incorporated into implementation of this plan.

Attachment X describes the values for assessment ratings used in the analysis, and the OPSEC analysis chart at Attachment X provides more information on the vulnerability and risk assessment.

7.1. Vulnerability: Non-secure (cell phone) communications systems are in use throughout ABC, Inc. Personnel use government-issued cell phones to coordinate travel, notify offices of current location and destination, pass unclassified mission information, and numerous other purposes. Cell phones are easily intercepted and can be used to target individuals, or information taken from these conversations could contribute to an analysis of operations and security vulnerabilities.

Countermeasure 1: OPSEC representatives in each work area will provide awareness training for their personnel immediately.

Countermeasure 2: Offices issuing cell phones to staff should examine the need for these phones and possible alternatives. The use of cell phones in place of short-range radios in some functions creates a potentially serious vulnerability, and replacement with secure radios should be considered. Even short-range radios with privacy encryption would be preferable to cell phones for such functions as security communications.

[USE THE FOLLOWING FORMAT FOR REMAINING VULNERABILITIES]

7.2. Vulnerability: (Below is a partial list of other potential vulnerabilities which may apply)

- Lack of OPSEC Awareness - - Personnel do not fully realize their OPSEC responsibilities. Employees are not aware of the extent to which an adversary depends on obtaining unclassified information on a defense project and their capability to decipher important intelligence data from this seemingly non-critical information.

- Testing - - subsystem testing may be vulnerable to exploitation.

- Open Source Literature - - Even unclassified information released to the news media, or at meetings, seminars, and through contractor advertisements, may provide analytical centers with valuable information regarding individual systems capabilities, limitations and technical operations.

- Communications - - All unsecured telephone conversations (including cellular phones) are vulnerable to monitoring, and all long-distance microwave transmissions are subject to intercept. Such vulnerabilities provide a source of information for intelligence agents. Communications supporting computer systems and faxes are equally vulnerable.

- Automated Information Systems (AIS) Operations - - The contract authorizes the use of AIS. Without adequate security measures, AIS are susceptible to intrusion or tampering through both hardware and software manipulation. Further, the emanations from AIS equipment and power lines may be subject to intercept. Electronic equipment such as word processors and electronic typewriters that are not TEMPEST approved, installed, and operated properly may produce emanations that are susceptible to intercept and exploitation.

- Visitor Control - - Visitors within the facility may observe or hear sensitive information, operations, or activities.

- Conference Room Security - - Classified and sensitive information could be compromised by covert listening devices installed in meeting rooms frequently used for sensitive discussions.

- Disgruntled Employees and Employees with Personal Problems (Adverse Information) - - Personnel possessing security clearances who, through personal adversities or circumstances such as marital difficulties, criminal behavior, excessive indebtedness, and/or indiscriminate use of alcohol, present attractive targets to Intelligence Services. Supervisors and/or fellow employees may become aware of these difficulties but may fail to notify management or security to investigate, electing to ignore the problem or rationalizing that some other party will take action.

Countermeasure:

8. TRAINING. All personnel will be informed of the requirements of this plan and their responsibilities as appropriate.

9. IMPLEMENTATION. All managers will comply with measures and procedures identified in this plan, and according to attachments.

Approved:

Date:

Annexes

Sensitive areas may require a separate annex to address vulnerabilities. Some functional areas of the organization may have unique vulnerabilities; address these unique vulnerabilities in a separate annex and limit distribution of the annex.

Attachments

Attachment 1. Hazard Consequence Table

Attachment 2. Definitions and Acronyms

Attachment 3. Threat Analysis

Attachment 4. Critical Information

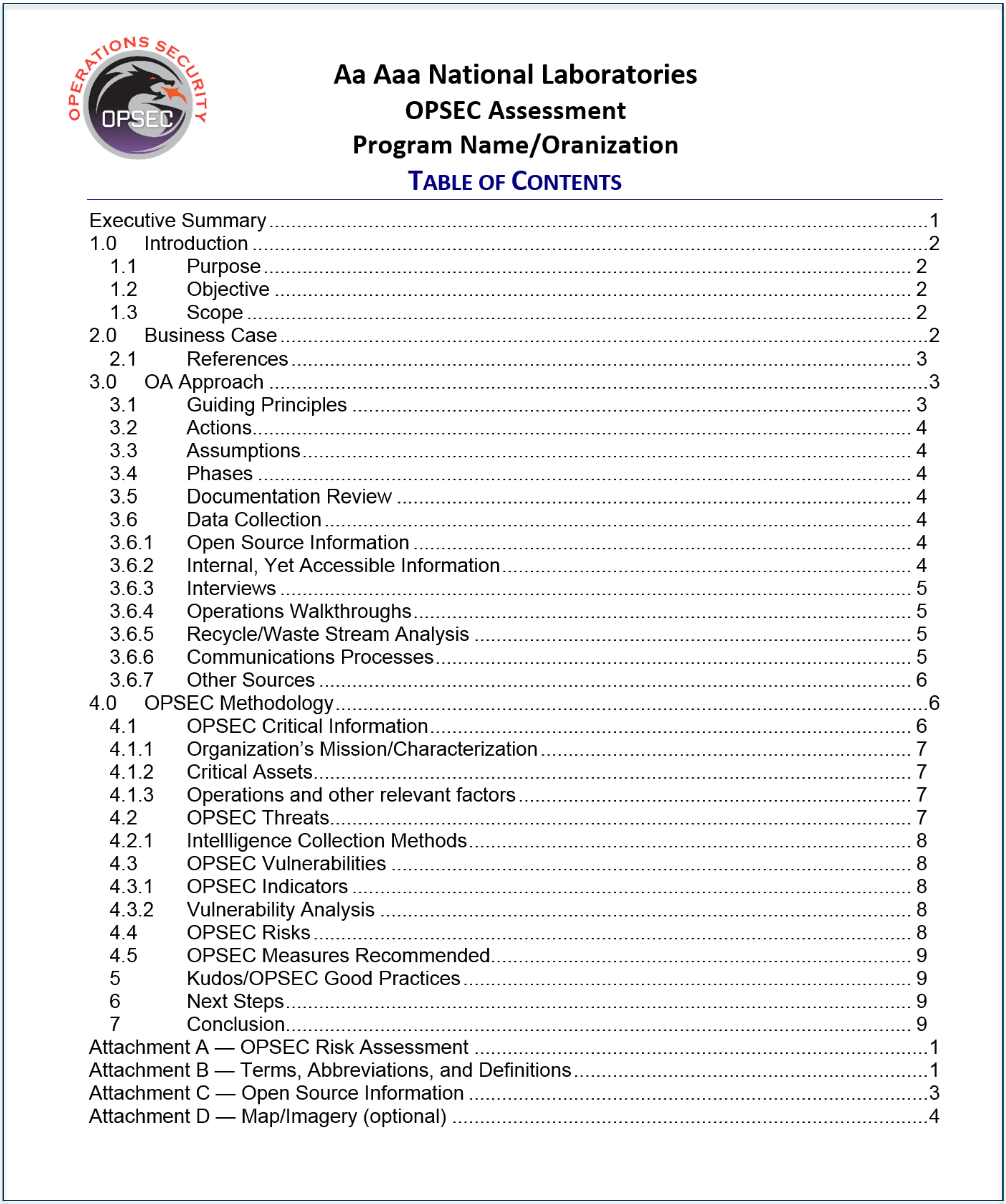
Attachment 5. Analysis Ratings Criteria

Attachment 6. OPSEC Analysis Chart

Appendix C: Sample OPSEC Assessment Report

An OA format should have, at a minimum, a cover page that includes document title, date (month/year conducted) and the overall classification of the report and an explanation of the activities associated with the OA to identify OPSEC concerns or vulnerabilities associated with the facility, project, or program. The activities associated with the OA can be outlined using:

- Observations
- Analysis and Discussion
- Recommendations



Aa Aaa National Laboratories

OPSEC Assessment

Program Name/Oranization

TABLE OF CONTENTS

Executive Summary 1

1.0 Introduction 2

1.1 Purpose 2

1.2 Objective 2

1.3 Scope 2

2.0 Business Case 2

2.1 References 3

3.0 OA Approach 3

3.1 Guiding Principles 3

3.2 Actions 4

3.3 Assumptions 4

3.4 Phases 4

3.5 Documentation Review 4

3.6 Data Collection 4

3.6.1 Open Source Information 4

3.6.2 Internal, Yet Accessible Information 4

3.6.3 Interviews 5

3.6.4 Operations Walkthroughs 5

3.6.5 Recycle/Waste Stream Analysis 5

3.6.6 Communications Processes 5

3.6.7 Other Sources 6

4.0 OPSEC Methodology 6

4.1 OPSEC Critical Information 6

4.1.1 Organization's Mission/Characterization 7

4.1.2 Critical Assets 7

4.1.3 Operations and other relevant factors 7

4.2 OPSEC Threats 7

4.2.1 Intellligence Collection Methods 8

4.3 OPSEC Vulnerabilities 8

4.3.1 OPSEC Indicators 8

4.3.2 Vulnerability Analysis 8

4.4 OPSEC Risks 8

4.5 OPSEC Measures Recommended 9

5 Kudos/OPSEC Good Practices 9

6 Next Steps 9

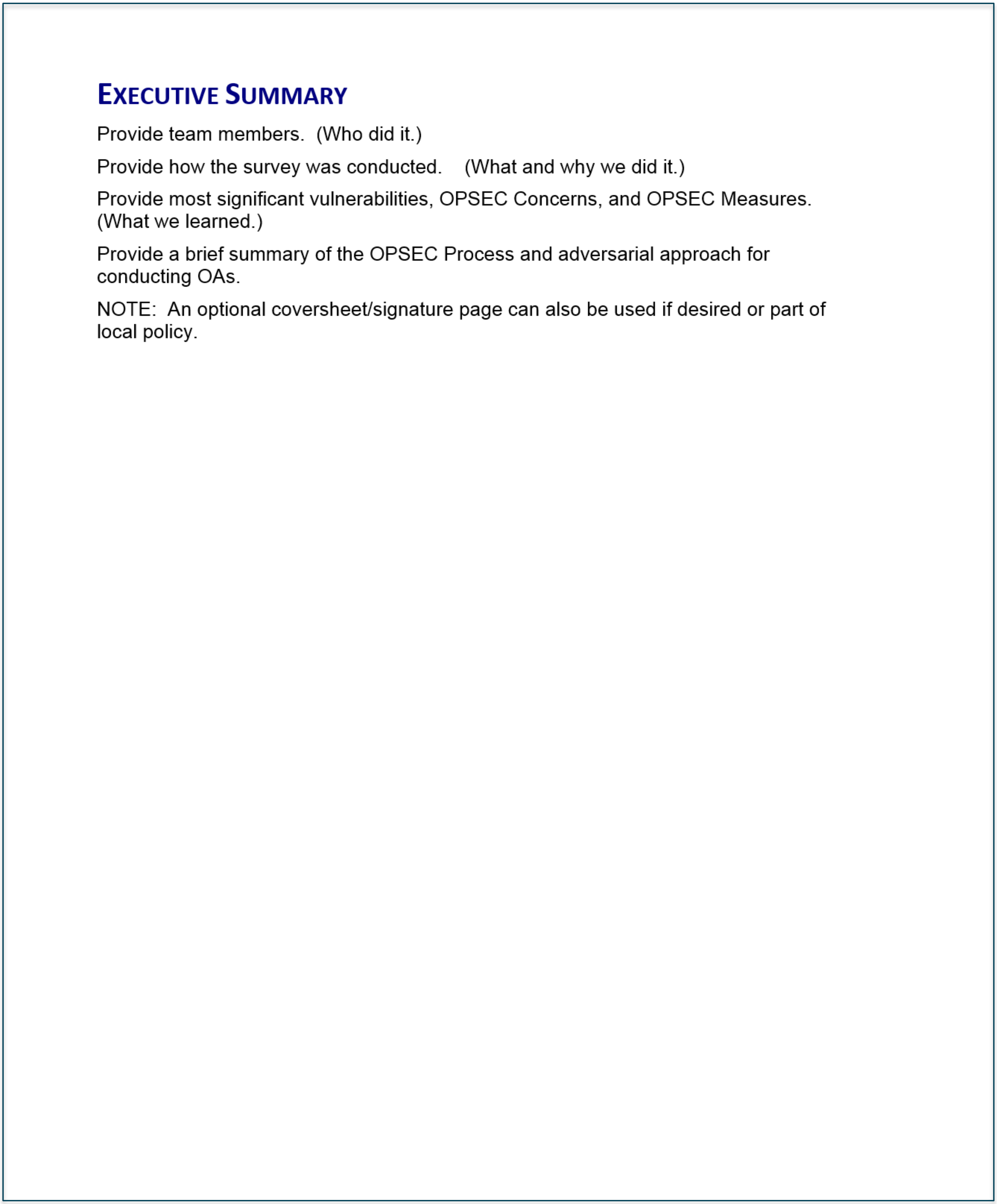
7 Conclusion 9

Attachment A — OPSEC Risk Assessment 1

Attachment B — Terms, Abbreviations, and Definitions 1

Attachment C — Open Source Information 3

Attachment D — Map/Imagery (optional) 4



Executive Summary

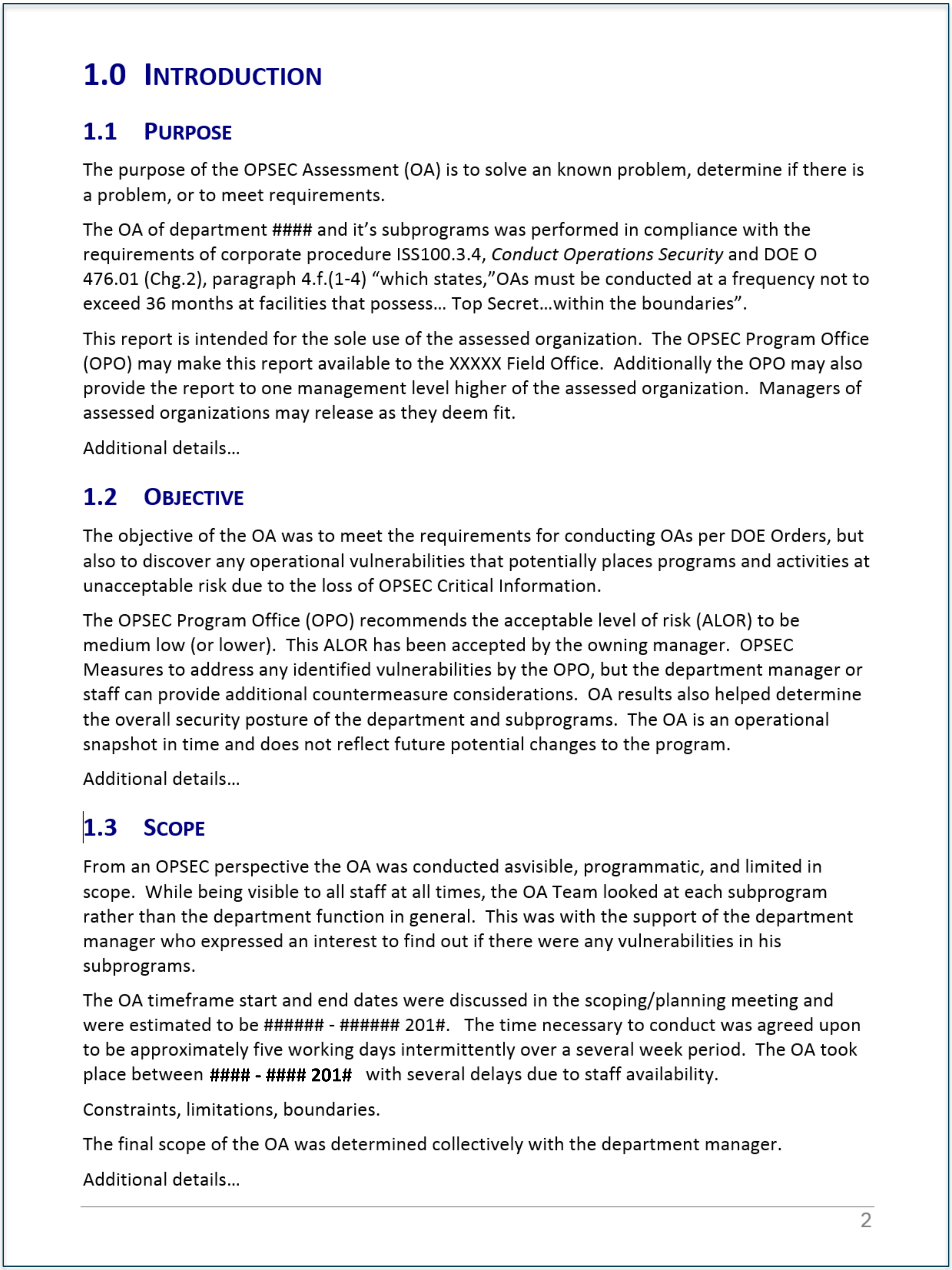
Provide team members. (Who did it.)

Provide how the survey was conducted. (What and why we did it.)

Provide most significant vulnerabilities, OPSEC Concerns, and OPSEC Measures. (What we learned.)

Provide a brief summary of the OPSEC Process and adversarial approach for conducting OAs.

NOTE: An optional coversheet/signature page can also be used if desired or part of local policy.



1.0 Introduction

1.1 Purpose

The purpose of the OPSEC Assessment (OA) is to solve an known problem, determine if there is a problem, or to meet requirements.

The OA of department #### and it’s subprograms was performed in compliance with the requirements of corporate procedure ISS100.3.4, *Conduct Operations Security* and DOE O 476.01 (Chg.2), paragraph 4.f.(1-4) “which states,”OAs must be conducted at a frequency not to exceed 36 months at facilities that possess… Top Secret…within the boundaries”.

This report is intended for the sole use of the assessed organization. The OPSEC Program Office (OPO) may make this report available to the XXXXX Field Office. Additionally the OPO may also provide the report to one management level higher of the assessed organization. Managers of assessed organizations may release as they deem fit.

Additional details…

1.2 Objective

The objective of the OA was to meet the requirements for conducting OAs per DOE Orders, but also to discover any operational vulnerabilities that potentially places programs and activities at unacceptable risk due to the loss of OPSEC Critical Information.

The OPSEC Program Office (OPO) recommends the acceptable level of risk (ALOR) to be medium low (or lower). This ALOR has been accepted by the owning manager. OPSEC Measures to address any identified vulnerabilities by the OPO, but the department manager or staff can provide additional countermeasure considerations. OA results also helped determine the overall security posture of the department and subprograms. The OA is an operational snapshot in time and does not reflect future potential changes to the program.

Additional details…

1.3 Scope

From an OPSEC perspective the OA was conducted asvisible, programmatic, and limited in scope. While being visible to all staff at all times, the OA Team looked at each subprogram rather than the department function in general. This was with the support of the department manager who expressed an interest to find out if there were any vulnerabilities in his subprograms.

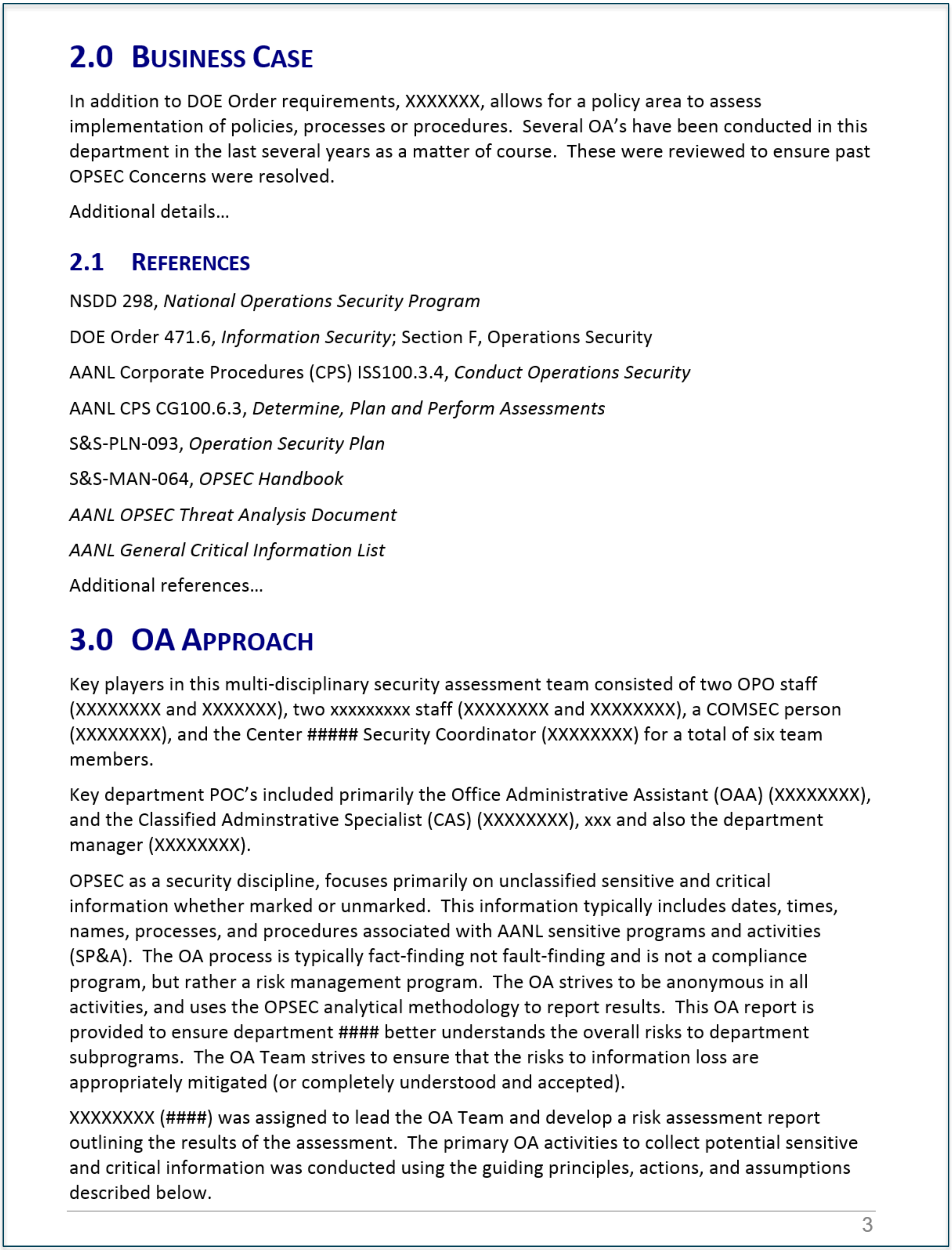
The OA timeframe start and end dates were discussed in the scoping/planning meeting and were estimated to be ###### - ###### 201#. The time necessary to conduct was agreed upon to be approximately five working days intermittently over a several week period. The OA took place between **#### - #### 201#** with several delays due to staff availability.

Constraints, limitations, boundaries.

The final scope of the OA was determined collectively with the department manager.

Additional details…

2



2.0 Business Case

In addition to DOE Order requirements, XXXXXXX, allows for a policy area to assess implementation of policies, processes or procedures. Several OA's have been conducted in this department in the last several years as a matter of course. These were reviewed to ensure past OPSEC Concerns were resolved.

Additional details...

2.1 References

NSDD 298, *National Operations Security Program*

DOE Order 471.6, *Information Security*; Section F, Operations Security

AANL Corporate Procedures (CPS) ISS100.3.4, *Conduct Operations Security*

AANL CPS CG100.6.3, *Determine, Plan and Perform Assessments*

S&S-PLN-093, *Operation Security Plan*

S&S-MAN-064, *OPSEC Handbook*

AANL OPSEC Threat Analysis Document

AANL General Critical Information List

Additional references...

3.0 OA Approach

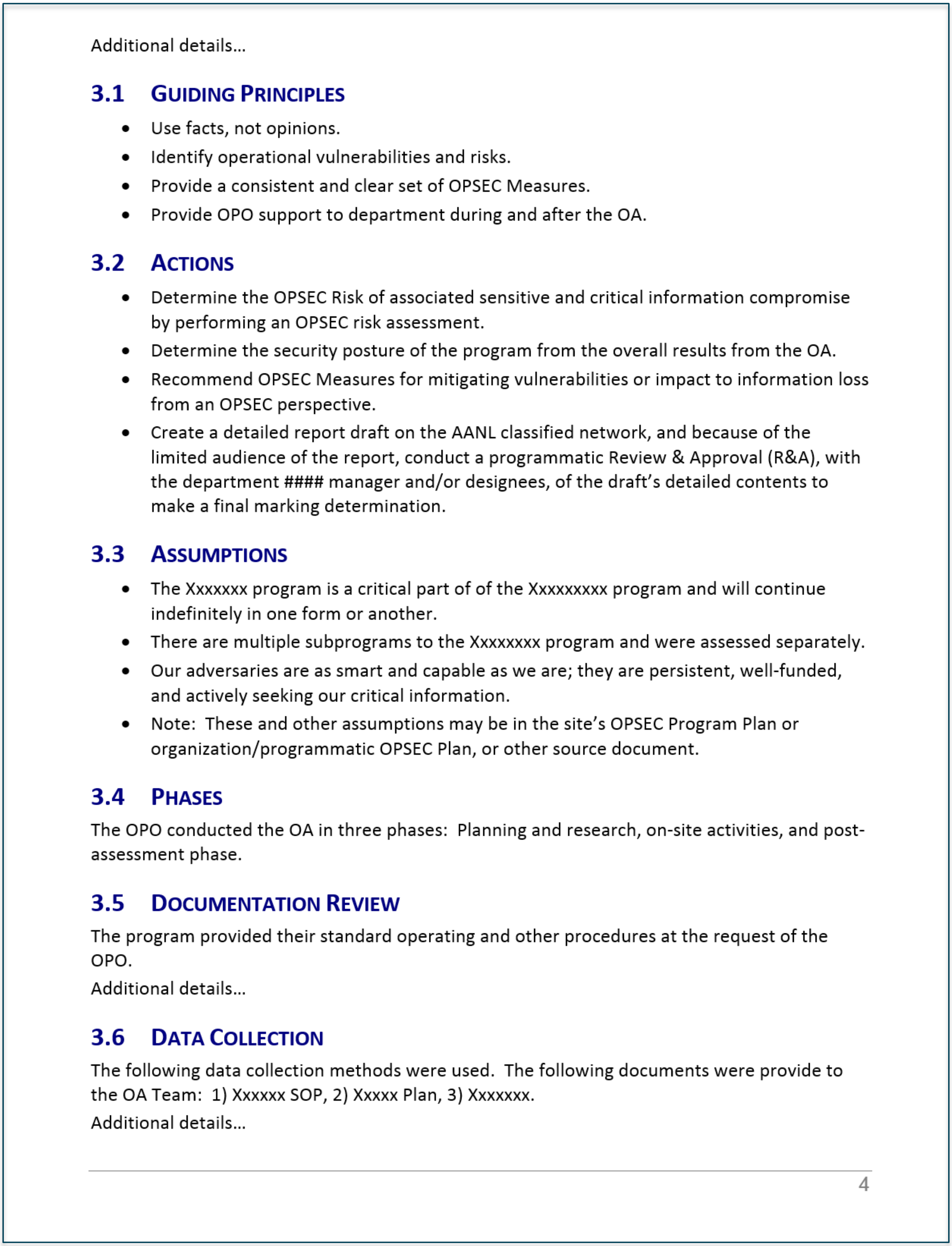
Key players in this multi-disciplinary security assessment team consisted of two OPO staff (XXXXXXXX and XXXXXXX), two xxxxxxxxx staff (XXXXXXXX and XXXXXXXX), a COMSEC person (XXXXXXXX), and the Center ##### Security Coordinator (XXXXXXXX) for a total of six team members.

Key department POC's included primarily the Office Administrative Assistant (OAA) (XXXXXXXX), and the Classified Adminstrative Specialist (CAS) (XXXXXXXX), xxx and also the department manager (XXXXXXXX).

OPSEC as a security discipline, focuses primarily on unclassified sensitive and critical information whether marked or unmarked. This information typically includes dates, times, names, processes, and procedures associated with AANL sensitive programs and activities (SP&A). The OA process is typically fact-finding not fault-finding and is not a compliance program, but rather a risk management program. The OA strives to be anonymous in all activities, and uses the OPSEC analytical methodology to report results. This OA report is provided to ensure department #### better understands the overall risks to department subprograms. The OA Team strives to ensure that the risks to information loss are appropriately mitigated (or completely understood and accepted).

XXXXXXXX (####) was assigned to lead the OA Team and develop a risk assessment report outlining the results of the assessment. The primary OA activities to collect potential sensitive and critical information was conducted using the guiding principles, actions, and assumptions described below.

3



Additional details…

3.1 Guiding Principles

- Use facts, not opinions.
- Identify operational vulnerabilities and risks.
- Provide a consistent and clear set of OPSEC Measures.
- Provide OPO support to department during and after the OA.

3.2 Actions

- Determine the OPSEC Risk of associated sensitive and critical information compromise by performing an OPSEC risk assessment.
- Determine the security posture of the program from the overall results from the OA.
- Recommend OPSEC Measures for mitigating vulnerabilities or impact to information loss from an OPSEC perspective.
- Create a detailed report draft on the AANL classified network, and because of the limited audience of the report, conduct a programmatic Review & Approval (R&A), with the department #### manager and/or designees, of the draft's detailed contents to make a final marking determination.

3.3 Assumptions

- The Xxxxxxx program is a critical part of of the Xxxxxxxxx program and will continue indefinitely in one form or another.
- There are multiple subprograms to the Xxxxxxxx program and were assessed separately.
- Our adversaries are as smart and capable as we are; they are persistent, well-funded, and actively seeking our critical information.
- Note: These and other assumptions may be in the site's OPSEC Program Plan or organization/programmatic OPSEC Plan, or other source document.

3.4 Phases

The OPO conducted the OA in three phases: Planning and research, on-site activities, and post-assessment phase.

3.5 Documentation Review

The program provided their standard operating and other procedures at the request of the OPO.

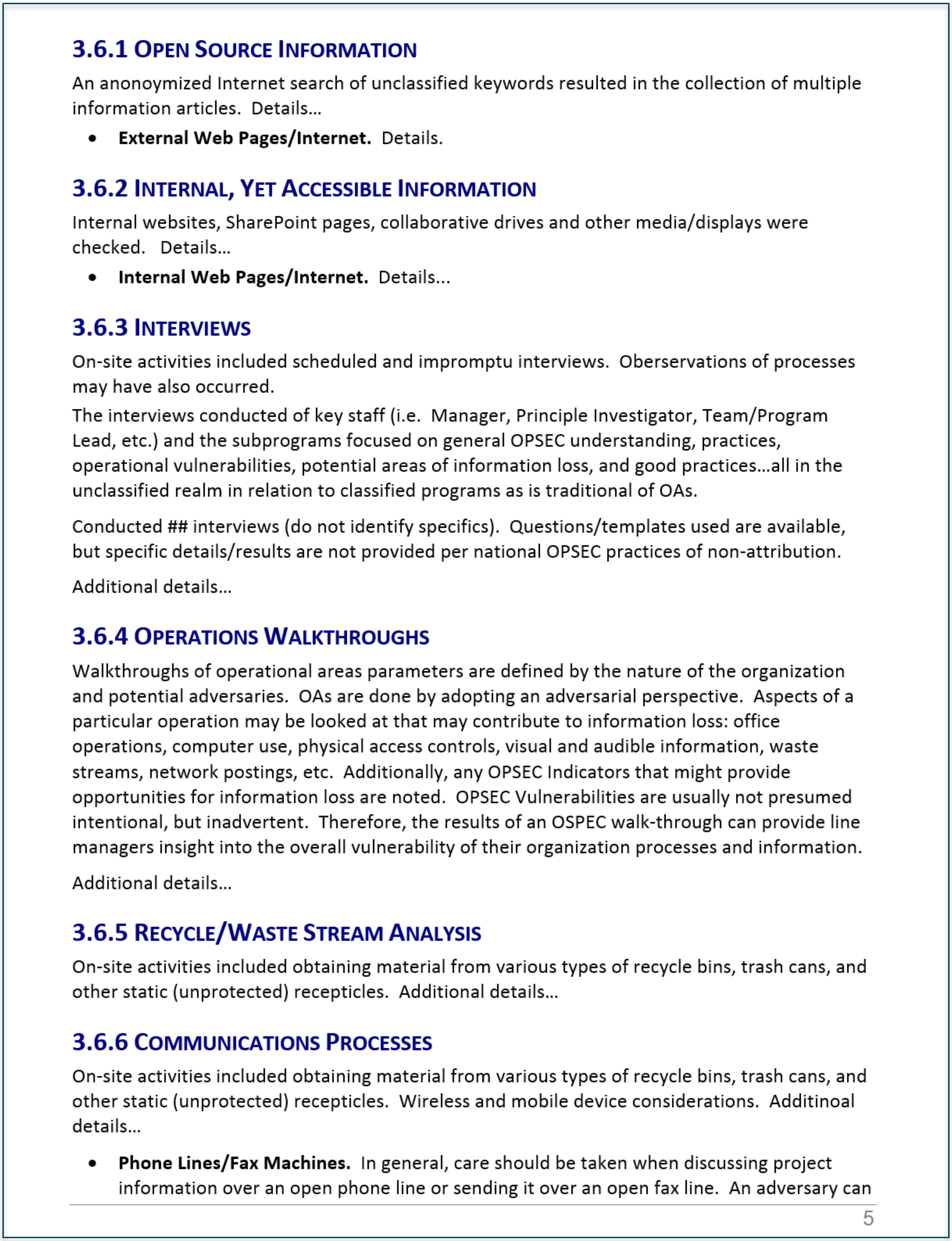
Additional details…

3.6 Data Collection

The following data collection methods were used. The following documents were provide to the OA Team: 1) Xxxxxx SOP, 2) Xxxxx Plan, 3) Xxxxxxx.

Additional details…

4



3.6.1 Open Source Information

An anonoymized Internet search of unclassified keywords resulted in the collection of multiple information articles. Details…

- **External Web Pages/Internet.** Details.

3.6.2 Internal, Yet Accessible Information

Internal websites, SharePoint pages, collaborative drives and other media/displays were checked. Details…

- **Internal Web Pages/Internet.** Details...

3.6.3 Interviews

On-site activities included scheduled and impromptu interviews. Oberservations of processes may have also occurred.

The interviews conducted of key staff (i.e. Manager, Principle Investigator, Team/Program Lead, etc.) and the subprograms focused on general OPSEC understanding, practices, operational vulnerabilities, potential areas of information loss, and good practices…all in the unclassified realm in relation to classified programs as is traditional of OAs.

Conducted ## interviews (do not identify specifics). Questions/templates used are available, but specific details/results are not provided per national OPSEC practices of non-attribution.

Additional details…

3.6.4 Operations Walkthroughs

Walkthroughs of operational areas parameters are defined by the nature of the organization and potential adversaries. OAs are done by adopting an adversarial perspective. Aspects of a particular operation may be looked at that may contribute to information loss: office operations, computer use, physical access controls, visual and audible information, waste streams, network postings, etc. Additionally, any OPSEC Indicators that might provide opportunities for information loss are noted. OPSEC Vulnerabilities are usually not presumed intentional, but inadvertent. Therefore, the results of an OSPEC walk-through can provide line managers insight into the overall vulnerability of their organization processes and information.

Additional details…

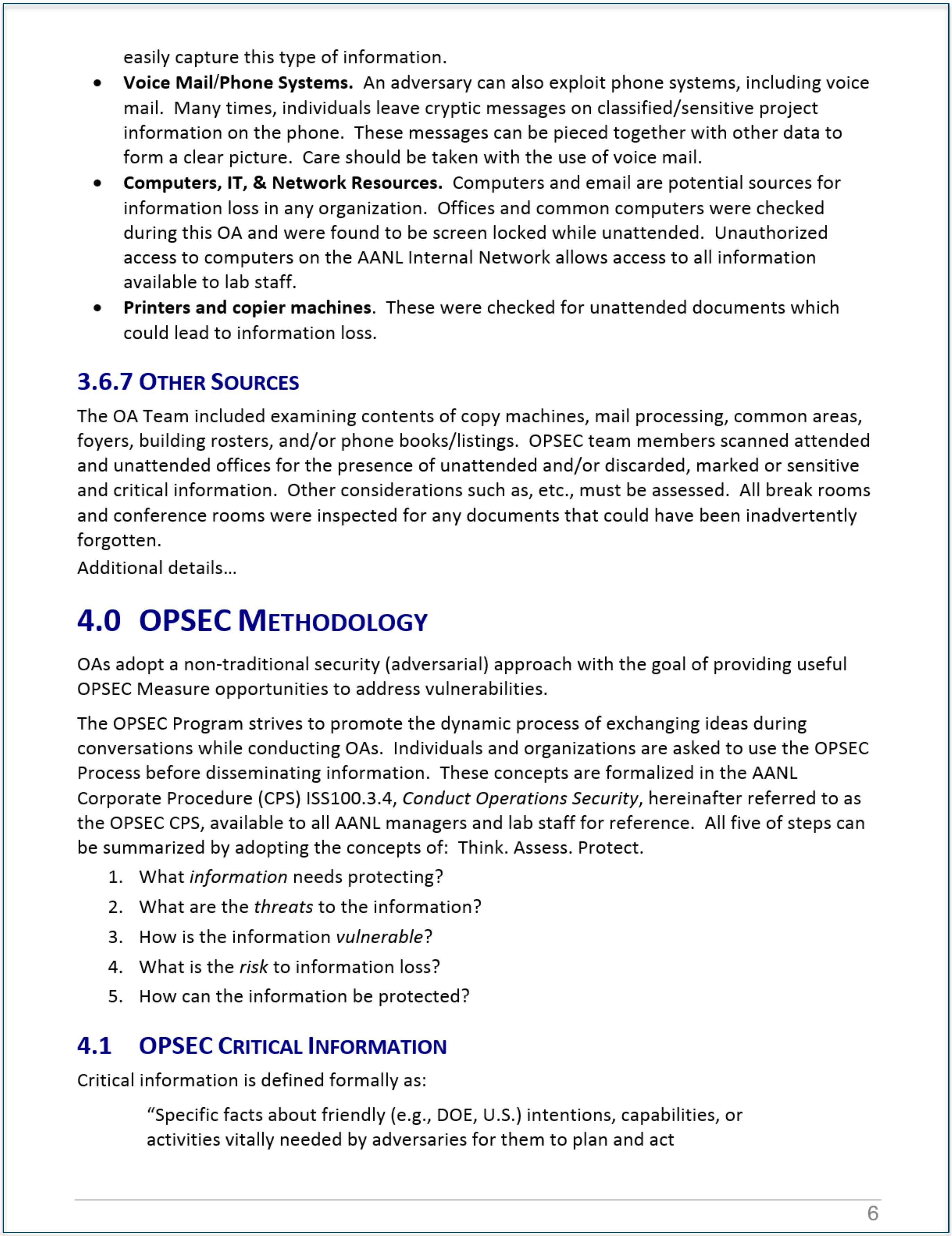
3.6.5 Recycle/Waste Stream Analysis

On-site activities included obtaining material from various types of recycle bins, trash cans, and other static (unprotected) recepticles. Additional details…

3.6.6 Communications Processes

On-site activities included obtaining material from various types of recycle bins, trash cans, and other static (unprotected) recepticles. Wireless and mobile device considerations. Additinoal details…

- **Phone Lines/Fax Machines.** In general, care should be taken when discussing project information over an open phone line or sending it over an open fax line. An adversary can



easily capture this type of information.

- **Voice Mail/Phone Systems.** An adversary can also exploit phone systems, including voice mail. Many times, individuals leave cryptic messages on classified/sensitive project information on the phone. These messages can be pieced together with other data to form a clear picture. Care should be taken with the use of voice mail.
- **Computers, IT, & Network Resources.** Computers and email are potential sources for information loss in any organization. Offices and common computers were checked during this OA and were found to be screen locked while unattended. Unauthorized access to computers on the AANL Internal Network allows access to all information available to lab staff.
- **Printers and copier machines**. These were checked for unattended documents which could lead to information loss.

3.6.7 Other Sources

The OA Team included examining contents of copy machines, mail processing, common areas, foyers, building rosters, and/or phone books/listings. OPSEC team members scanned attended and unattended offices for the presence of unattended and/or discarded, marked or sensitive and critical information. Other considerations such as, etc., must be assessed. All break rooms and conference rooms were inspected for any documents that could have been inadvertently forgotten.

Additional details…

4.0 OPSEC Methodology

OAs adopt a non-traditional security (adversarial) approach with the goal of providing useful OPSEC Measure opportunities to address vulnerabilities.

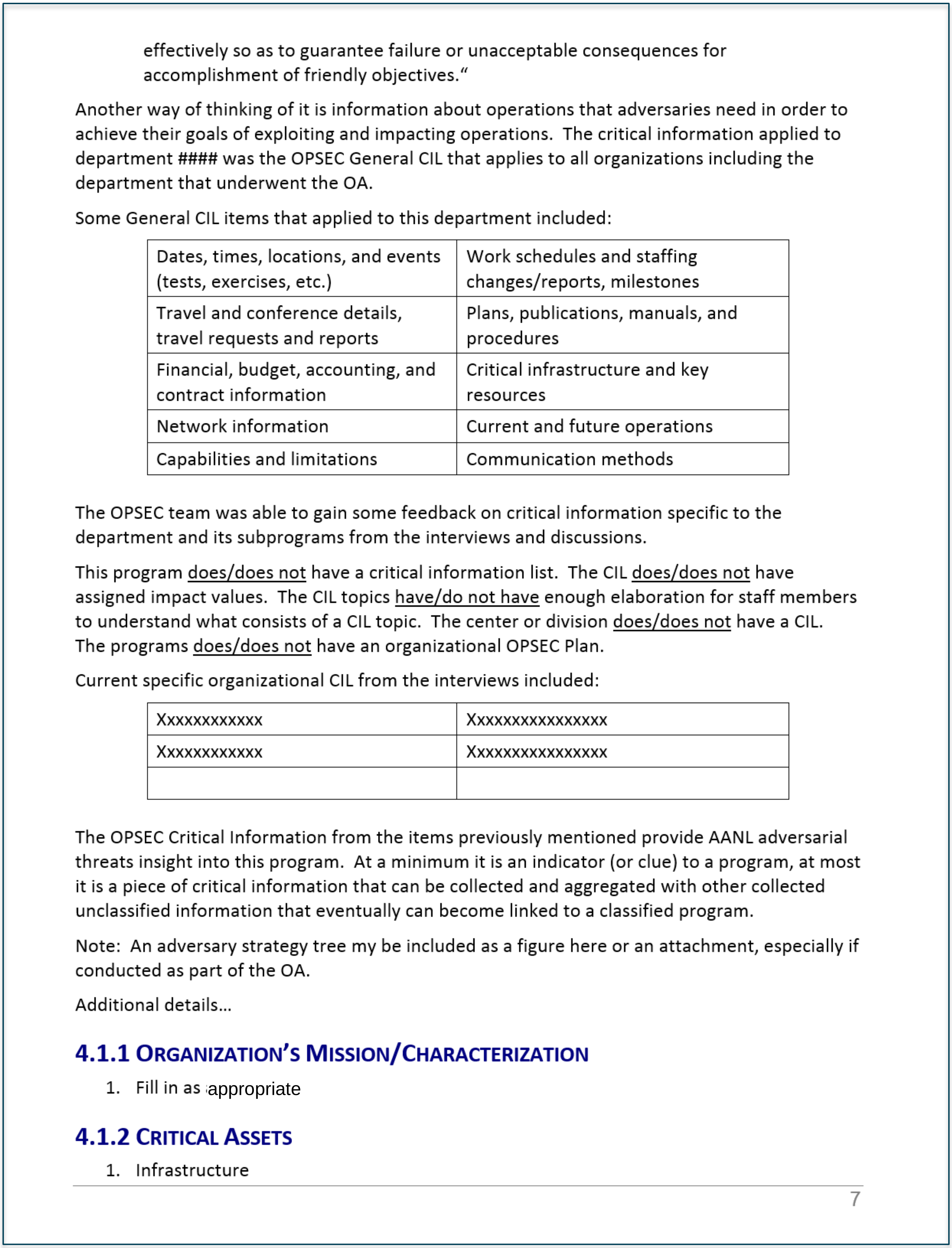
The OPSEC Program strives to promote the dynamic process of exchanging ideas during conversations while conducting OAs. Individuals and organizations are asked to use the OPSEC Process before disseminating information. These concepts are formalized in the AANL Corporate Procedure (CPS) ISS100.3.4, *Conduct Operations Security*, hereinafter referred to as the OPSEC CPS, available to all AANL managers and lab staff for reference. All five of steps can be summarized by adopting the concepts of: Think. Assess. Protect.

1. What *information* needs protecting?
2. What are the *threats* to the information?
3. How is the information *vulnerable*?
4. What is the *risk* to information loss?
5. How can the information be protected?

4.1 OPSEC Critical Information

Critical information is defined formally as:

> “Specific facts about friendly (e.g., DOE, U.S.) intentions, capabilities, or activities vitally needed by adversaries for them to plan and act



> effectively so as to guarantee failure or unacceptable consequences for accomplishment of friendly objectives."

Another way of thinking of it is information about operations that adversaries need in order to achieve their goals of exploiting and impacting operations. The critical information applied to department #### was the OPSEC General CIL that applies to all organizations including the department that underwent the OA.

Some General CIL items that applied to this department included:

Dates, times, locations, and events (tests, exercises, etc.)	Work schedules and staffing changes/reports, milestones
Travel and conference details, travel requests and reports	Plans, publications, manuals, and procedures
Financial, budget, accounting, and contract information	Critical infrastructure and key resources
Network information	Current and future operations
Capabilities and limitations	Communication methods

The OPSEC team was able to gain some feedback on critical information specific to the department and its subprograms from the interviews and discussions.

This program does/does not have a critical information list. The CIL does/does not have assigned impact values. The CIL topics have/do not have enough elaboration for staff members to understand what consists of a CIL topic. The center or division does/does not have a CIL. The programs does/does not have an organizational OPSEC Plan.

Current specific organizational CIL from the interviews included:

Xxxxxxxxxxxx	Xxxxxxxxxxxxxxxx
Xxxxxxxxxxxx	Xxxxxxxxxxxxxxxx

The OPSEC Critical Information from the items previously mentioned provide AANL adversarial threats insight into this program. At a minimum it is an indicator (or clue) to a program, at most it is a piece of critical information that can be collected and aggregated with other collected unclassified information that eventually can become linked to a classified program.

Note: An adversary strategy tree my be included as a figure here or an attachment, especially if conducted as part of the OA.

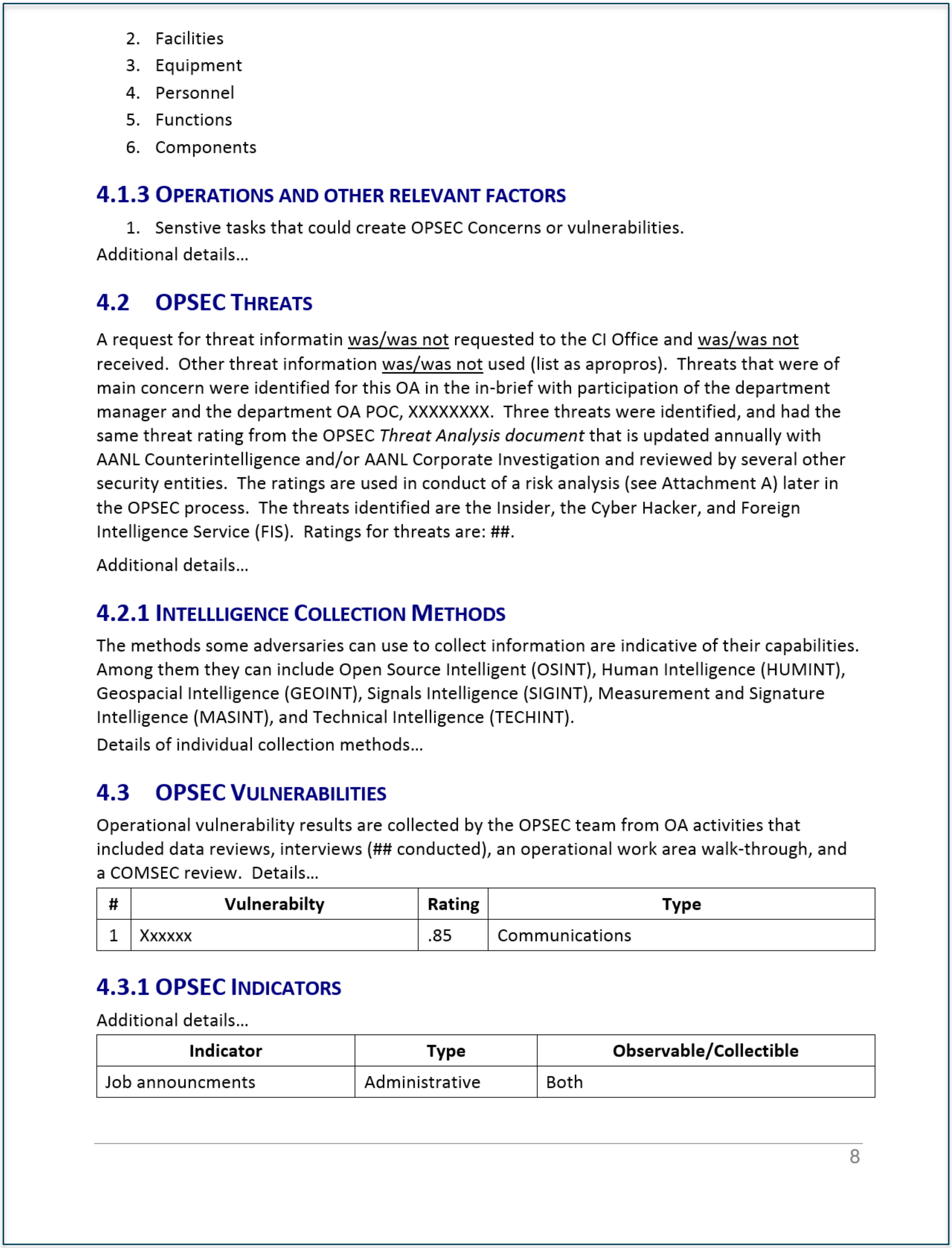
Additional details…

4.1.1 Organization's Mission/Characterization

1. Fill in as appropriate

4.1.2 Critical Assets

1. Infrastructure



2. Facilities
3. Equipment
4. Personnel
5. Functions
6. Components

4.1.3 Operations and other relevant factors

1. Senstive tasks that could create OPSEC Concerns or vulnerabilities.

Additional details…

4.2 OPSEC Threats

A request for threat informatin was/was not requested to the CI Office and was/was not received. Other threat information was/was not used (list as apropros). Threats that were of main concern were identified for this OA in the in-brief with participation of the department manager and the department OA POC, XXXXXXXX. Three threats were identified, and had the same threat rating from the OPSEC *Threat Analysis document* that is updated annually with AANL Counterintelligence and/or AANL Corporate Investigation and reviewed by several other security entities. The ratings are used in conduct of a risk analysis (see Attachment A) later in the OPSEC process. The threats identified are the Insider, the Cyber Hacker, and Foreign Intelligence Service (FIS). Ratings for threats are: ##.

Additional details…

4.2.1 Intellligence Collection Methods

The methods some adversaries can use to collect information are indicative of their capabilities. Among them they can include Open Source Intelligent (OSINT), Human Intelligence (HUMINT), Geospacial Intelligence (GEOINT), Signals Intelligence (SIGINT), Measurement and Signature Intelligence (MASINT), and Technical Intelligence (TECHINT).

Details of individual collection methods…

4.3 OPSEC Vulnerabilities

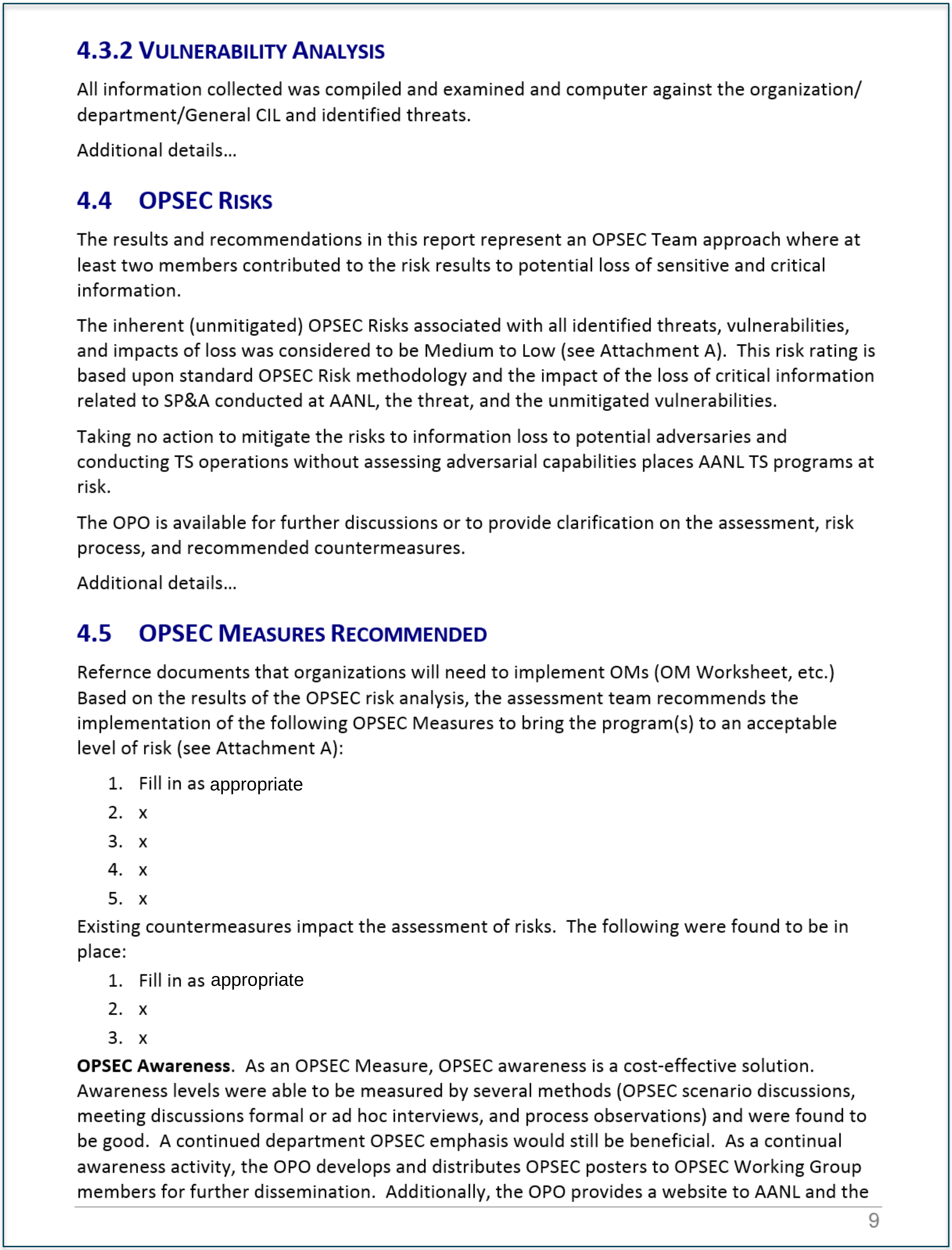
Operational vulnerability results are collected by the OPSEC team from OA activities that included data reviews, interviews (## conducted), an operational work area walk-through, and a COMSEC review. Details…

#	Vulnerabilty	Rating	Type
1	Xxxxxx	.85	Communications

4.3.1 OPSEC Indicators

Additional details…

Indicator	Type	Observable/Collectible
Job announcments	Administrative	Both



4.3.2 Vulnerability Analysis

All information collected was compiled and examined and computer against the organization/ department/General CIL and identified threats.

Additional details…

4.4 OPSEC Risks

The results and recommendations in this report represent an OPSEC Team approach where at least two members contributed to the risk results to potential loss of sensitive and critical information.

The inherent (unmitigated) OPSEC Risks associated with all identified threats, vulnerabilities, and impacts of loss was considered to be Medium to Low (see Attachment A). This risk rating is based upon standard OPSEC Risk methodology and the impact of the loss of critical information related to SP&A conducted at AANL, the threat, and the unmitigated vulnerabilities.

Taking no action to mitigate the risks to information loss to potential adversaries and conducting TS operations without assessing adversarial capabilities places AANL TS programs at risk.

The OPO is available for further discussions or to provide clarification on the assessment, risk process, and recommended countermeasures.

Additional details…

4.5 OPSEC Measures Recommended

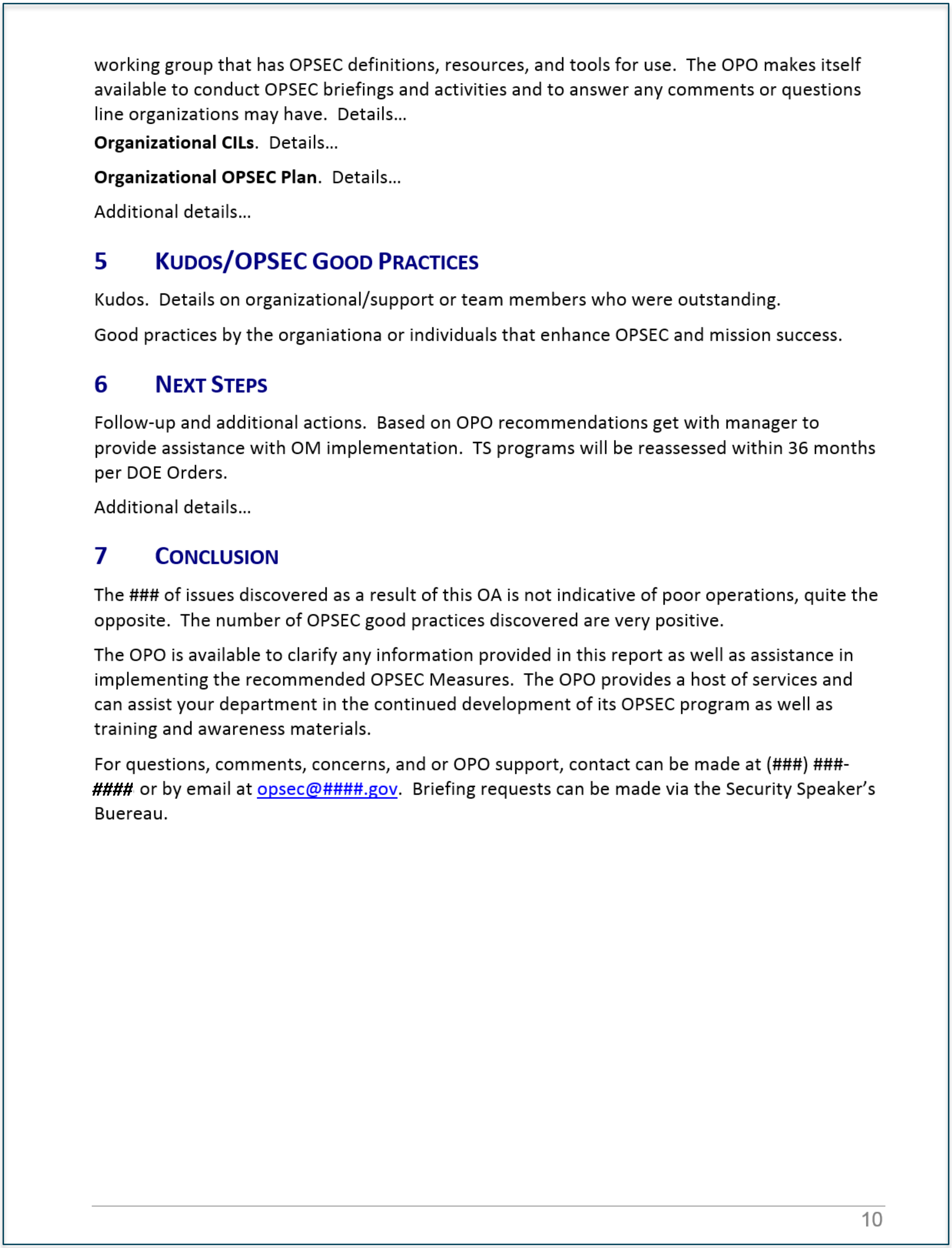
Refernce documents that organizations will need to implement OMs (OM Worksheet, etc.) Based on the results of the OPSEC risk analysis, the assessment team recommends the implementation of the following OPSEC Measures to bring the program(s) to an acceptable level of risk (see Attachment A):

1. Fill in as appropriate
2. x
3. x
4. x
5. x

Existing countermeasures impact the assessment of risks. The following were found to be in place:

1. Fill in as appropriate
2. x
3. x

OPSEC Awareness. As an OPSEC Measure, OPSEC awareness is a cost-effective solution. Awareness levels were able to be measured by several methods (OPSEC scenario discussions, meeting discussions formal or ad hoc interviews, and process observations) and were found to be good. A continued department OPSEC emphasis would still be beneficial. As a continual awareness activity, the OPO develops and distributes OPSEC posters to OPSEC Working Group members for further dissemination. Additionally, the OPO provides a website to AANL and the



working group that has OPSEC definitions, resources, and tools for use. The OPO makes itself available to conduct OPSEC briefings and activities and to answer any comments or questions line organizations may have. Details…

Organizational CILs. Details…

Organizational OPSEC Plan. Details…

Additional details…

5 Kudos/OPSEC Good Practices

Kudos. Details on organizational/support or team members who were outstanding.

Good practices by the organiationa or individuals that enhance OPSEC and mission success.

6 Next Steps

Follow-up and additional actions. Based on OPO recommendations get with manager to provide assistance with OM implementation. TS programs will be reassessed within 36 months per DOE Orders.

Additional details…

7 Conclusion

The ### of issues discovered as a result of this OA is not indicative of poor operations, quite the opposite. The number of OPSEC good practices discovered are very positive.

The OPO is available to clarify any information provided in this report as well as assistance in implementing the recommended OPSEC Measures. The OPO provides a host of services and can assist your department in the continued development of its OPSEC program as well as training and awareness materials.

For questions, comments, concerns, and or OPO support, contact can be made at (###) ###-#### or by email at opsec@####.gov. Briefing requests can be made via the Security Speaker's Buereau.

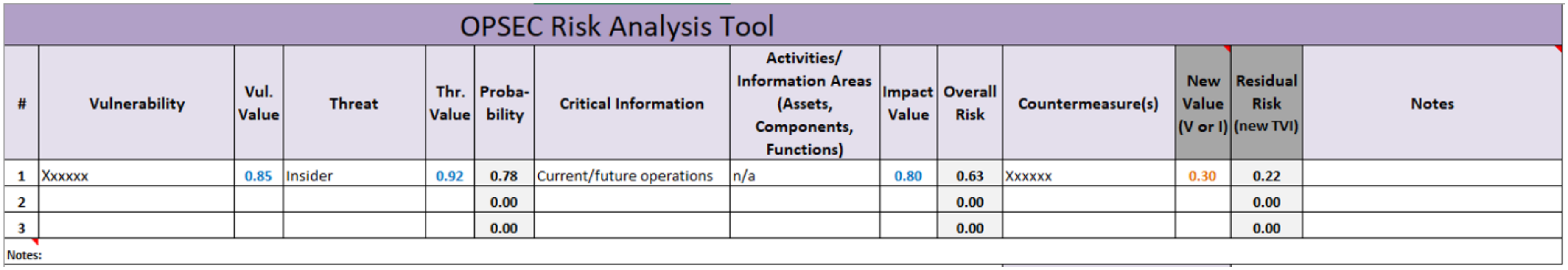
ATTACHMENT A — OPSEC RISK ASSESSMENT

OVERVIEW

The AANL OPSEC Risk Assessment Matrix consists of:

- Insider Threat (risk ratings include FIS and Cyber Hackers)

IDENTIFIED OPSEC THREATS: INSIDER THREAT (MALICIOUS, UNWITTING, ETC.)



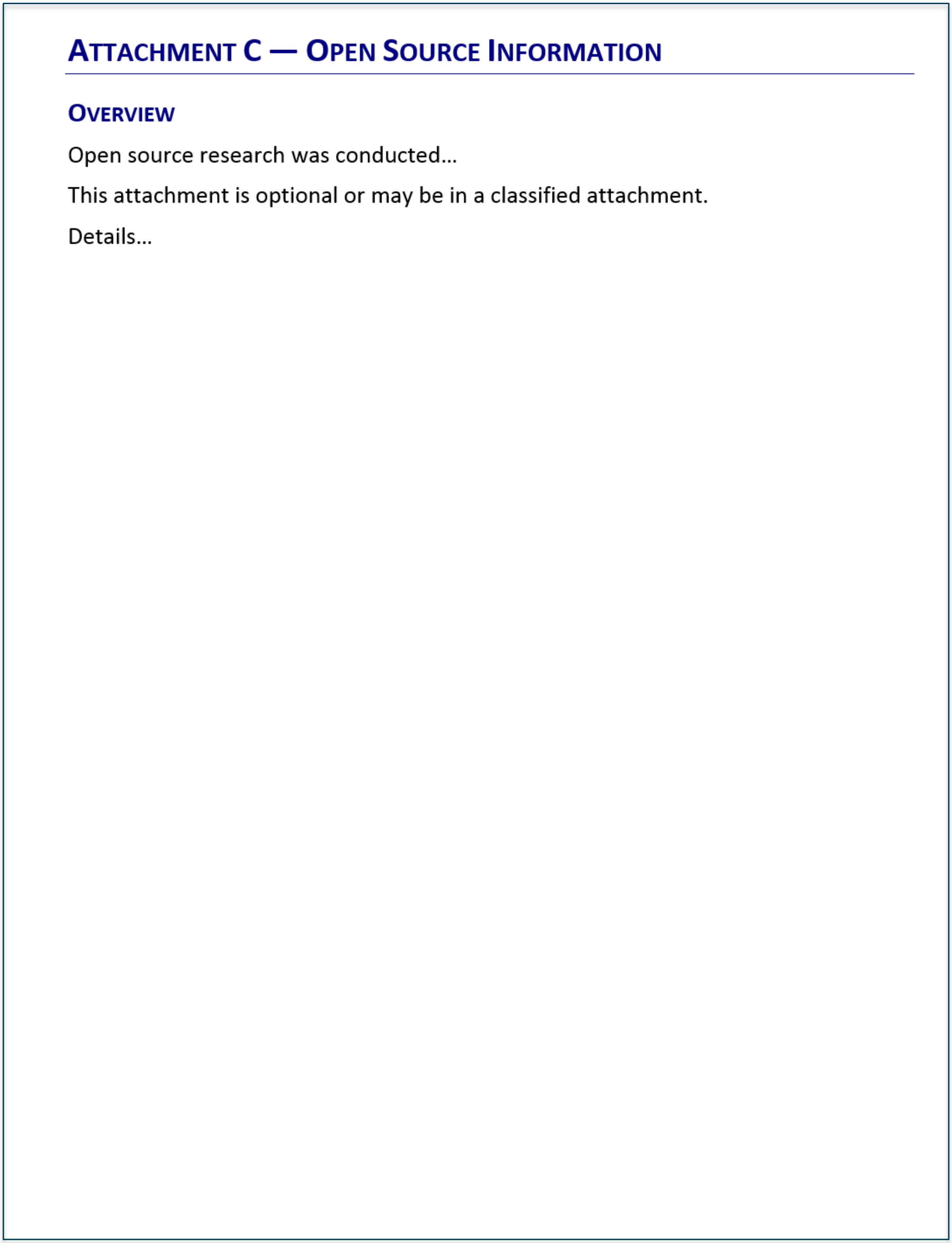
OPSEC Risk Analysis Tool

#	Vulnerability	Vul. Value	Threat	Thr. Value	Proba-bility	Critical Information	Activities/ Information Areas (Assets, Components, Functions)	Impact Value	Overall Risk	Countermeasure(s)	New Value (V or I)	Residual Risk (new TVI)	Notes
1	Xxxxxx	0.85	Insider	0.92	0.78	Current/future operations	n/a	0.80	0.63	Xxxxxx	0.30	0.22	
2					0.00				0.00			0.00	
3					0.00				0.00			0.00	
Notes:													

Figure 1. OPSEC Risk Analysis Tool Table

Attachment B — Terms, Abbreviations, and Definitions

Term	Definition



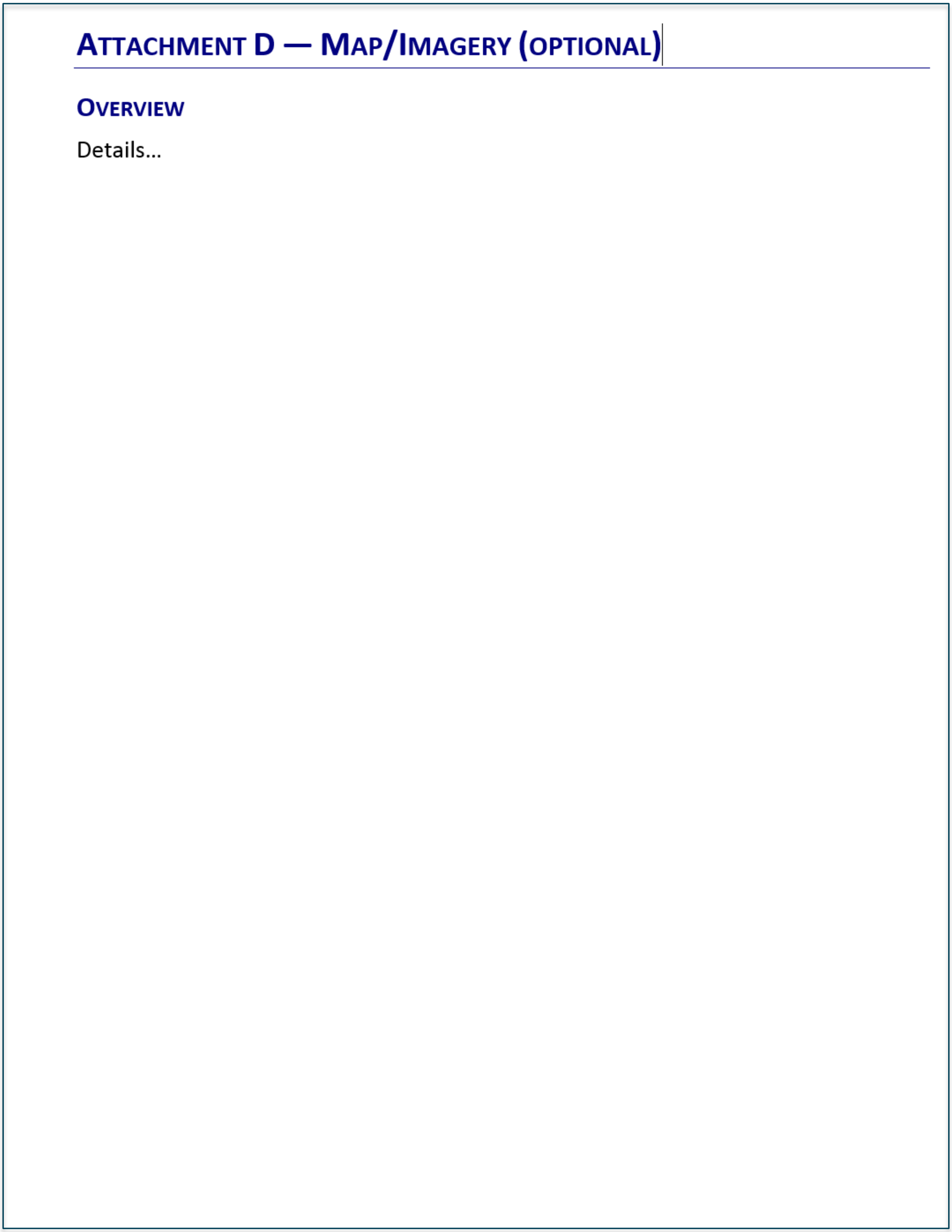
Attachment C — Open Source Information

Overview

Open source research was conducted…

This attachment is optional or may be in a classified attachment.

Details…



ATTACHMENT D — MAP/IMAGERY (OPTIONAL)

OVERVIEW

Details…

Appendix D: Sample Threat Statement

HYPOTHETICAL NATIONAL LABORATORY (HNL) OPSEC THREAT STATEMENT

EXECUTIVE SUMMARY
Overall, the threat to site mission, personnel, and assets is Low/Medium/High. HNL is now faced with adversaries that have demonstrated both intent and capability to obtain critical information and assets. A detailed analysis of the threat to HNL is provided in Attachment 3. The following is a summary of this analysis: ____

THREAT/ADVERSARY TYPES
HNL is currently threatened by the following adversary types: Terrorists, Criminals, Psychotics, Violent Activists, Insiders and Intelligence Collectors. Specific and known individuals and/or groups that have been determined to pose an OPSEC threat to HNL's critical information are contained in the classified Counterintelligence Threat Assessment, which is not a part of this Threat Statement, and available through the HNL CI Office, (555) 555-1234. An unclassified analysis of known adversary types that are currently in operation in the vicinity of HNL is as follows:

____

COLLECTION TECHNIQUES
The aforementioned Adversary Types have been known to employ the following collection techniques to obtain critical information: HUMINT, SIGINT, IMINT, MASINT, OSINT, TRASHINT and Cyber/Social Engineering attacks. Specifically, the adversary ___(fill in)___________________.

TARGETS
According to Counterintelligence estimates, adversaries may focus their intelligence collection efforts on the following friendly targets at HNL:____

THREAT LEVEL

	LOW	MEDIUM-LOW	MEDIUM	MEDIUM-HI	HIGH
Terrorists				X	
Criminals					X
Psychotics		X			
Activists			X		
Insiders					X
Intel Collectors				X	

This threat level matrix assigns a particular threat level to each adversary type, based on the latest DOE Counterintelligence estimate for the region encompassing Hypothetical National Laboratory (HNL).

CONCLUSION
____
____

Appendix E: Sample Website Reviews

OPSEC WEBSITE REVIEW

Website Owner: ___________________________
Contact Info: ______________________________

Webmaster: _______________________________
Contact Info: ______________________________

OPSEC Website Reviewer(s): ____
Date(s) of Review: ____
Website URL: ____
___ External/Public Website ___ Internal Website

Internet Protocol (IP) range: ____
Security Technologies used: ____
Remote Access Security: ____
Cybersecurity Training: ____
Password Requirements: ____
Current CICO[1] Threat: ____
Webpages reviewed: ____
____
____
____
Critical Information Observed: ____
Articles reviewed: ____
____
____
____
Critical Information Observed: ____
____
____
____

[1] Computer Intrusion for Collection Operations – directed cyberattacks for the purpose of collecting information

Appendix F: IOSS OPSEC Program Implementation Tiers

Interagency OPSEC Support Staff

The words “OPSEC Program” mean many things to many people. The IOSS characterizes three types of OPSEC Programs, based primarily on the degree of commitment on the part of leadership, and the resources and expectations dedicated to the OPSEC Program. These are described below. An estimate of resources necessary to support each tier is provided following the tier descriptions.

To really make OPSEC work for your organization, you need to have at least a Tier Two program. If you’re only doing Tier One OPSEC, you’ve got eye wash; you might as well not waste your time.

OPSEC only works if you make an investment to change the culture of your organization. To do that, you need time and resources to first understand the threat, and then to help your people understand it. Once you understand the threat, you can start to make OPSEC work for you. But threat analysis and awareness training take time, which is the one commodity most of us are short of.

What that means is that commanders and managers must put the emphasis on a culture shift to make OPSEC important, and to make it important up front, before the action starts. OPSEC isn’t a good Band-Aid. OPSEC isn’t even a good tourniquet. You have to integrate an OPSEC mindset into every mission activity in your organization, from the beginning. Before supplies are ordered, procedures are implemented, orders are passed, or coordination is begun, your staff must understand their vulnerabilities and what to do about them. Most of the intelligence in the world is collected from open source. Why? Because we can’t -- or don’t -- protect our critical information. We don’t even know how badly we’re being had because our adversaries can hide in the woodwork. They can anonymously capture our most precious secrets from the internet. They can call us on the phone and we’ll tell them. We give them access to our business, to our infrastructure, and to our families. Not on purpose, but it’s all out there.

Without a commitment to do OPSEC, and not just talk about it, we’re only making ourselves feel good. An OPSEC program is more than appointing an OPSEC officer and making a list of critical information. You have to do awareness training. You have to assess your vulnerabilities and measure the risks, and decide which ones to fix. Then you have to fix them. You have to go back and assess them again, and again, and again. You have to make policies and establish procedures, then slap wrists when they’re ignored or forgotten. You have to get people to buy into the idea that we do have secrets to keep, and they’re important to our very survival. You have to remind people, when a crisis occurs and the adrenaline starts to flow, that they still need to practice OPSEC. You have to be there, in their face, to say slow down, think, and be careful. You can’t do that on a part time basis.

So, OPSEC is either important, or it isn’t. A plan isn’t worth the paper it’s written on if you don’t do it. Being right on paper isn’t good enough. You have to be right in the trenches, too.

- Tier One programs satisfy all the minimum administrative requirements for having an OPSEC program. Tier One programs are generally adequate to satisfy IG requirements. There is a minimal commitment to actually implementing OPSEC or integrating the OPSEC process into mission activities.
  - An OPSEC officer has been appointed and received basic OPSEC training. The OPSEC officer is part time, generally committing less than 30% of available duty hours to OPSEC.

  - A policy has been published.
  - A working group has been appointed by senior management, and is convened periodically.
  - A critical information list is published.
  - Awareness training is accomplished annually.

- Tier Two programs are actively pursuing implementation of OPSEC measures in daily operations, but the OPSEC officer is part time (less than 60% of duty hours), and resources dedicated to OPSEC are limited. In addition to meeting Tier One standards, these programs have achieved the following characteristics:

  - The OPSEC officer maintains a Continuity Book, and has a Program Plan which is updated annually.
  - The OPSEC Working Group meets at least quarterly.
  - Senior leadership is actively involved in the program and regularly endorses OPSEC measures to the staff.
  - OPSEC coordinators are appointed, trained, and actively involved in each functional area of the organization.
  - The OPSEC officer maintains documentation required to make use of end-of-year money.
  - An OPSEC survey or assessment is conducted at least annually.
  - The OPSEC officer has established adequate contacts to provide viable, useful intelligence threat information.

- Tier Three programs have the benefit of adequate resources to meet organizational OPSEC requirements, and have the full support and participation of senior leadership. In addition to Tier Two standards, these programs have achieved the following characteristics:

  - The OPSEC officer commits 70% to 100% of duty hours to the OPSEC program.
  - The OPSEC officer has established an extensive network of contacts who provide intelligence threat assessment, ideas on program management, and who can provide consultation or mentoring support should a situation require assistance.
  - The OPSEC awareness program reaches all new employees within 30 days of assignment, and awareness program activities (multi-media clips, posters, automated reminders) involve every employee at least once quarterly.
  - The OPSEC officer either publishes a periodic newsletter, or contributes to another publication on a regular basis.
  - The OPSEC officer conducts and documents OPSEC program self-inspections on a regular basis.
  - An OPSEC survey or assessment is conducted at least once annually. Senior leadership tracks implementation of approved countermeasures resulting from the assessment or survey.
  - OPSEC is incorporated into local exercises and is included in emergency or contingency responses. The OPSEC officer is part of the emergency or contingency response team, or has input to the team.
  - The OPSEC officer participates in web content management, or has provided training for web content managers.
  - The OPSEC program has an adequate training budget for awareness training materials, and for working group members and OPSEC coordinators.
  - There is an organizational policy on the use of secure communications and/or restrictions on use of unencrypted communications in specific situations.

OPSEC Program Resource Guide

	Tier One	Tier Two	Tier Three
Leadership involvement			
Occasional (briefing, chair meeting, publish letter)	●		
Regular & recurring (staff meetings, all-hands calls, etc.)		●	●
Program Development			
OPSEC Officer: IOSS Associates Program (40 hours at IOSS)		●	●
Working Group members: IOSS Associates Program (40 hours at IOSS)		●	●
Leadership: Policy coordination, authority delegation, plan coordination (20 hrs.)		●	●
Manpower			
OPSEC Officer: 10 to 12 hours per week	●		
OPSEC Officer: Average 17 hours per week		●	
OPSEC Officer(s): 30 to 60 hours per week			●
Working Group members: Average 2 hours monthly	●	●	●
OPSEC Coordinators: Average 5 hours weekly		●	
OPSEC Coordinators: Average 10 hours weekly			●
Training			
OPSEC Officer: 40 hours (OPSE-380 or equivalent)	●	●	●
OPSEC Officer: 24 hours advanced course			●
Working Group members: 4 hours (OPSE-1301 or equivalent)	●	●	
Working Group members: 8 hours (OPSE-1301 or equivalent + briefings)			●
OPSEC Coordinators: 8 hours (OPSE-300 or equivalent)		●	●
Awareness			
30 minutes annually for all staff	●		
60 minutes annually for all staff		●	
30 to 60 minutes orientation for all staff within 60 days of assignment		●	●
30 minutes quarterly for all staff			●
O&M Funding Estimates			
TDY: OPSEC Officer(s) training 1 week + airfare x # people; average $900/person (more overseas)	●	●	●
TDY: OPSEC Officer & Working Group members to Associates Program 1 week + airfare x # people; average $900/person (more overseas)		●	●
TDY: Two analysts to assist with OPSEC survey 10 days + airfare x 2 people; average $3,200 (more overseas)		●	●
TDY: OPSEC Officer(s) attend conference or continuation training 1 week + airfare + fees/tuition x # people; average $1,200/person		●	●
Training and awareness materials (variable)		●	
Implementation of countermeasures identified by survey(s); Est $10-40K			●

We’re getting radical at the IOSS. We’ve come to understand over the years that training and videos aren’t enough. If we train thirty people, who leave at the end of the course individually enlightened but not empowered to do anything, what have we achieved? If we distribute thousands of videos, but nothing changes, what have we achieved? To be a change agent, we have to cultivate an OPSEC culture, and help those who come to us for assistance understand how to do something with the tools we provide. So here’s a radical idea: let’s focus on programs. Let’s build an infrastructure that can use the knowledge and expertise we help you develop.

Our focus now is on programs. Training is designed to help you understand the process so that you can do OPSEC. Having at least a Tier Two program, or being committed to building one, will soon be a prerequisite to manpower-intensive IOSS services, like mobile training teams, OPSEC survey assistance, and eligibility for the IOSS Associates Program. The wide variety of IOSS products, web-based training, computer-based training, events, and classroom courses will remain available to all government and government contractor customers. The IOSS is a relatively small staff, and our resources are finite. Our task is huge. We need to communicate better, work with the community, understand your needs, and set standards that are fair to everyone to ensure the ultimate success of our mission. We think we’re headed in the right direction, and we hope you agree.

U.S. DEPARTMENT OF ENERGY
OPERATIONS SECURITY