

Applying OPSEC to Government Acquisitions and Contracts



www.iooss.gov

June 2011

Applying OPSEC To Government Acquisitions and Contracts

TABLE OF CONTENTS

OPSEC and Acquisition

OPSEC – A Primer

- What is OPSEC?

- The OPSEC Process

 - Analysis of Threats

 - Identify Critical Information

 - Analysis of Vulnerabilities

 - Risk Assessment

 - Application of Appropriate Countermeasures

Overview of DoD Acquisition (A Convergence of Systems and Critical Information)

The DoD Acquisition Management System (DAMS)

- Material Solution Analysis Phase (MSA)

- Technology Development Phase (TD)

- Engineering and Manufacturing Development Phase (EMD)

- Production and Deployment Phase (PD)

- Operations and Support Phase (OS)

OPSEC Requirements in DoD Contracts

- Pre Contract Award

- Contract Documentation

- Contract Security Classification Specification (DD254)

- Post Contract Award

OPSEC Program, Plans and Assessments

- Organizational OPSEC Program

- Organizational OPSEC Plan

- Program OPSEC Plan

- OPSEC Assessments

Conclusion

Message from the Director, Interagency OPSEC Support Staff

OPSEC and Acquisition

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 United State's national objectives. By design, government acquisition processes must maintain a level of transparency in order 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 Office of the National Counterintelligence Executive (ONCIX) reports,

“... 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.”¹ (emphasis added)

In 2005 The FBI arrested a Kentucky maintenance mechanic, leading to a conviction of conspiracy to commit trade secret theft, for selling more than 800 blueprints of his company's innovative equipment for making liquid crystal displays worth an estimated \$100 M to a foreign-based rival.² 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.”³

The General Accounting Office (GAO) reports the cost to the Department of Defense (DoD) of schedule delays [independent of cause] in 95 weapons systems programs in 2007 was \$4.9M 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!

“Developing new technologies ensures we remain competitive in modern economic and military arenas, but only if we protect the fruits of our labor.”⁴ Operations Security (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.

¹ FY2008 Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, 23 July 2009, NCIX-007-09, Office of the National Counterintelligence executive (ONCIX).

² Federal Bureau of Investigation, http://www.fbi.gov/page2/June06/company_spy061906.htm

³ FBI Special Agent Mark Thompson, Federal Bureau of Investigation, http://www.fbi.gov/page2/June06/company_spy061906.htm

⁴ A national advantage through R&D”, Averbek and Jones, March 11, 2010, <http://www.rdmag.com/News/2010/03/Averbek-Jones-research-development-funding-A-national-advantage-through-R-D/>

OPSEC ----- A PRIMER

What is OPSEC?

The patterns and routines in day-to-day activities, such as those defined by the Defense Acquisition Management System (DAMS), present a background against which critical information may be revealed to an adversary. Critical information is defined in DODM 5205.02 as,

“Critical Information is information about DoD activities, intentions, capabilities, or limitations that an adversary seeks in order to gain a military, political, diplomatic, economic, or technological advantage. Such information, if revealed to an adversary, may prevent or degrade mission accomplishment, cause loss of life, or damage friendly resources.”⁵

The OPSEC process provides a systematic approach to addressing the protection of critical information and supplements the effectiveness of traditional security practices such as physical, personnel, communications and cybersecurity. OPSEC differs from traditional security in that it is specifically tailored to each program and is constantly evolving to degrade an adversary’s ability to predict or disrupt sensitive activities through the protection of generally unclassified information.

OPSEC is essentially a “mindset” that raises awareness among all program personnel that adversaries of the U.S. actively seek unclassified information (i.e. critical information) as well as classified information which may provide them with a strategic or tactical advantage against the U.S. Eliminating, or minimizing, indicators of classified or sensitive activity when planning to acquire new capabilities will serve to impede foreign intelligence objectives.

It is important to note, the application of OPSEC practices rarely affects whether an activity will occur, such as first article testing, manufacturing process demonstrations or system disposal. OPSEC does affect how an activity occurs. The OPSEC process is most cost effective when fully integrated early in the acquisition process and evolves as a program matures in response to changes in the threat environment.

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.

⁵ Department of Defense Manual, Number 5205.02-M, Appendix 1 to Enclosure 3, page 12, November 3, 2008.

Through the OPSEC process it is possible to:

1. Identify critical information requiring protection.
2. Analyze threats and vulnerabilities which may be exploited to reveal critical information.
3. Determine appropriate OPSEC measures to protect critical information.

The OPSEC Process

The OPSEC process consists of five basic steps: Analysis of Threat, Identification of Critical Information, Analysis of Vulnerabilities, Assessment of Risk, and Application of Appropriate Countermeasures. For clarity of explanation, the OPSEC process is assumed to be a sequential process. During actual application of the process the first two steps may occur simultaneously, require frequent review and are critical inputs to the remaining three steps. In all cases OPSEC is a continuous process.



The OPSEC Process

Step 1: Analysis of Threats

“America must not ignore the threat gathering against us. Facing clear evidence of peril, we cannot wait for the final proof, the smoking gun that could come in the form of a mushroom cloud.”- President George W. Bush

Threat analysis is an examination of an adversary’s technical and operational capabilities, motivation, and intentions to detect and exploit vulnerabilities leading to the discovery of critical information.

The world is constantly changing and the same is true of the threat. As a world leader, the U.S. is a principal target for the exploitation of its technology⁶ and the DoD 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 U.S. 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 which may be obtained from U.S. Intelligence Agencies or local law enforcement organizations and is **always a critical component of a well written OPSEC Plan.**

Reviewing the traditional intelligence cycle provides a foundation for understanding the composite intelligence threat to critical information. The process inherent in the cycle applies equally to all intelligence systems including those of foreign nation intelligence services; economic competitors; or ad hoc efforts by narcotraffickers or terrorist groups.



Traditional Intelligence Cycle⁷

⁶ “Targeting U.S. Technologies: A Trend analysis of reporting from Defense Industry 2009”, Defense Security Service, 2010

⁷ http://www.public-domain-content.com/books/cia_factbook_on_intelligence

Planning and Direction – Intelligence systems are normally tasked to collect and assess information in response to key leadership questions relative to intent and capability. The answers to such questions require information about the opponent and are key to an adversary’s operational or policy decisions. In the OPSEC methodology this information may be considered “Critical Information” that must be protected through OPSEC measures to ensure U.S. operations and technological advantages are maintained.

Examples of acquisition related questions an adversary might want to know include: What technologies is the U.S. investing in, and at what levels? What is the status of a particular technology development and when might it be deployed by the U.S.? What is a particular corporation’s marketing strategy for a newly developed product(s)? Where are the technical weaknesses in a new product?

B. Collection – An adversary’s intelligence collectors determine where, and how, the answers to their leadership questions can best be collected. Commonly, the answers to key questions are not found in one location or discovered through a single collection method.

For example, Internet research might reveal the development of a new leading edge technology at a corporation (Open Source Intelligence, 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, HUMINT) and intercepted telephone conversations between a sales representative and government personnel may reveal the level of interest in the technology (Signals Intelligence, 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.

C. Processing – Once information is obtained it is processed and becomes an input for intelligence analysis enroute to becoming finished intelligence.

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.

D. Analysis and Production – Following initial processing, information is evaluated in terms of the credibility and the reliability of the source(s). It is compared with previously obtained data to form intelligence profiles. An intelligence analyst may fill information gaps with reasoned assumptions based upon expertise and experience leading to the production of finished intelligence.

Examples of analysis of acquisition related information may include the consideration of the source of the data (i.e. the Vice President of Marketing at a known government contractor, postings on corporate websites, news reports), the validity of the data (i.e. how many sources are

reporting the information), and does the data make sense when considering previously revealed information.

E. Dissemination - Dissemination is the communication of finished intelligence to the adversary's leadership. Dissemination may take many forms such as formal written reports, verbal presentations, email, phone calls, etc. 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.

It is essential to the success of the OPSEC process that all adversaries be identified, and their intentions and capabilities evaluated. In almost every government acquisition, a threat analysis provided by the Government will serve as the basis for identifying adversaries, and contractors will generally rely upon that threat analysis and local area threat information available from sources such as the FBI, local police, and local military intelligence activities to develop an OPSEC Plan. Ideally, prior to supporting a government acquisition, the contractor organization (e.g., corporation) will already have an overarching Organization OPSEC Plan in place.

Additional information on intelligence collection disciplines is available at www.iooss.gov / Library Resources/ Operations Security Joint Publication 3-13.3, 29 June 2006/ APPENDIX A.

Step 2: Identify Critical Information

*“When the well’s dry, we know the worth of water.”
- Benjamin Franklin,
Inventor and American Statesman*

The OPSEC process is designed to protect critical information. Critical information consists of data about an organization's intentions, capabilities, or activities that must be shielded from an adversary in order to maintain significant military, economic, political, or technological advantage. Therefore, any compilation of critical information must be viewed from two perspectives – Yours and the adversary's!

The common characteristics of a good Critical Information List (CIL) include:

- ✓ Input from all organizational participants involved in the activity or acquisition.
- ✓ Easy to understand and widely distributed **within** the organization.
- ✓ Consists of an appropriate number of items dependent upon the complexity and sensitivity of the task.
- ✓ In concert with higher level critical information lists as approved by senior leadership.
- ✓ Dated and periodically reviewed.
- ✓ Unclassified.

Examples of critical information related to government acquisitions may include unique engineering and manufacturing processes; computer network descriptions, technology

development or unique application(s), advanced or fundamental research efforts, delivery dates and locations.

Step 3 Analysis of Vulnerabilities

“...if September 11 taught us anything, it taught us that we're vulnerable, and vulnerable in ways that we didn't fully understand.” - Condoleezza Rice, Secretary of State

Determining vulnerabilities involves a systematic and comprehensive analysis of an operation, activity or acquisition conducted by the primary and supporting organizations **as it might be viewed through the eyes of an adversary**. Any action that can be observed, data that can be interpreted, or the aggregation thereof must be identified relative to the critical information it may reveal.

Once the intent and capabilities of the adversary are known (threat), and critical information has been identified, a vulnerability analysis is conducted to determine the existence of indicators of vulnerability. Indicators are observable actions that adversaries can interpret or aggregate, to reach conclusions or estimates of critical or classified information revealing intentions, capabilities or activities.

Bottom line: **A vulnerability is an exploitable weakness.**

OPSEC is primarily focused upon the necessary peripheral actions and events that support an acquisition, but which may also provide an indicator to an adversary of a vulnerability which may be exploited. Examples of acquisition vulnerabilities may include: Unusual contract requirements, excessively detailed background information in a Statement of Work (SoW), unusual material requisitions, significantly increased prime and subcontractor communications, unusual test and evaluation activities and special delivery requirements.

An expanded list of potential indicators is provided at www.iooss.gov / Library Resources/ Operations Security Joint Publication 3-13.3, 29 June 2006/ APPENDIX B.

Step 4 Risk Assessment

*“Risk is a part of God's game, alike for men and nations.”
- Warren Buffett, American businessman*

The OPSEC Risk Assessment step brings together all of the data from the previous OPSEC steps to provide a holistic picture of the OPSEC environment. It is where the probability and programmatic impact of the adversary's success in acquiring and exploiting critical information is determined. **The Risk Assessment step provides indispensable input to the eventual selection of appropriate OPSEC measures.**

OPSEC risk assessments create a ***priority*** listing of the recognized risks to critical information

And form

a basis for the identification of ***potential*** OPSEC measures.

As previously discussed, the OPSEC process is continuous, requiring periodic re-evaluation of critical information, threats, vulnerabilities and OPSEC measures. It is critical, in recognition of resource limitations, that the cost and effectiveness of OPSEC measures be accurately and systematically measured. Potential OPSEC measures costs include the funding, manpower and time, etc. required to implement a proposed measure. Effectiveness of an OPSEC measure is portrayed as the anticipated reduction of OPSEC risk as a result of the measure.

Once an OPSEC measure has been implemented, effectiveness is portrayed as the actual reduction of OPSEC risk, known as the residual risk, which provides feedback for future OPSEC measure decisions. The effectiveness of OPSEC measures should be periodically re-evaluated with senior leadership as a part of an annual OPSEC Assessment.

OPSEC risk assessments create benchmarks for the future measurement of risk mitigation as the result of ***implemented*** OPSEC measures.

The determination of risk in the OPSEC process requires a degree of subjective decision-making based on the best available estimates of an adversary's threat, our own recognized vulnerabilities and the impact of the loss of critical information to U.S. government operations, activities or acquisitions. OPSEC Risk may be represented by the simple function:

OPSEC Risk Calculation

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

Where:

Threat = A measure (or assessment) of an adversary's intent and capability to acquire critical information (OPSEC process step 1).

Vulnerability = A measure (or assessment) of the existence of indicators and technical vulnerabilities to adversary intelligence collection methods (OPSEC process step 3).

Impact = The internal assessment of the impact the loss of critical information will have upon the successful completion of U.S. government activities, operations or acquisitions (OPSEC process step 2).

If an identified threat, vulnerability or adverse impact to the success of the activity or operation exists, a value must be assigned (either numerical or subjective). The higher the value, the more serious the threat, vulnerability or impact. The assigned rating is normalized on a scale of zero to one (numerically) or may be a descriptive rating (none, low, medium-low, medium, medium-high, high) using a rating criteria such as this can be found at www.iooss.gov / Library Resources/ Operations Security Joint Publication 3-13.3, 29 June 2006/ APPENDIX C.

If there is no threat, vulnerability or impact of loss of information, a value of zero, or, "none" will be assigned. In this case, THERE IS NO OPSEC RISK and OPSEC measures DO NOT need to be applied.

For example, using the DODM 5202.02M matrices referenced above, an acquisition for a newly developed ship propulsion system which will provide the U.S. with a distinct advantage in a wartime operation may be of interest to a number of potential adversaries. The threat against the information is measured based upon intelligence as to the intent and capabilities of known adversaries. If, for example, an adversary's intent to acquire the critical information is deemed, "HI" but the intelligence collection capability is assessed as, "MED HI" then the overall threat to the critical information is deemed, "MED HI".

Assuming technology is not classified and therefore may not be sufficiently protected through traditional security practices, a vulnerability may exist. For example, discussions amongst

professional colleagues at industry conferences, or communications with company shareholders may provide the adversary with insight into the Government's acquisition. Thus, the acquisition Program Manager (PM) may determine that vulnerabilities exist and assign a, "MED" value to this element of risk.

The probability of critical information loss is calculated by multiplying the threat by the vulnerability. In this example, using the matrices provided in DODM 5205.02M, the probability of critical information loss is equal to the Threat (MED HI) times the Vulnerability (MED), or "MED."

As the final step in the Risk Assessment process, the subjectively assessed value of the critical information is cross-referenced with the probability of critical information loss. In this example, the assessed impact of loss to the government is, "HI." Using the Risk Assessment Table in DODM 5205.02-M the overall risk assessment may then be determined as, "MED."

The above process should be repeated for each item of identified critical information against each form of threat and yield a prioritized Critical Information List (CIL) based upon the overall OPSEC risk to critical information. This list should be used to focus the determination and selection of OPSEC measures in the next step of the OPSEC process.

Step 5 Application of Appropriate OPSEC Measures

*"If you have a fire, you don't want to – at that point – start buying fire trucks and training people."
[In reference to the 2010 Gulf Oil Spill]
--Yossi Sheffi, Director MIT Engineering Systems Division*

The fifth step of the OPSEC process is the selection and application of OPSEC measures. Appropriate OPSEC measures include anything that effectively mitigates an adversary's ability to exploit vulnerabilities and can be applied in accordance with senior level guidance as to the acceptable level of cost and OPSEC risk. Therefore, it may not be necessary that an OPSEC measure entirely eliminate a vulnerability.

The most effective OPSEC measures are usually simple, straightforward, procedural adjustments that effectively eliminate or minimize the generation of indicators. When considering OPSEC measures, it is important to recognize that **the application of OPSEC measures themselves may also lead to the generation of new indicators of vulnerability** in an acquisition or program. For this reason, the OPSEC process is dynamic and periodic assessments are necessary to ensure proper and cost effective OPSEC measures remain in place when necessary.

The selection of specific OPSEC measures should follow a simple cost-benefit decision by senior leadership based upon the data generated in the preceding Risk Analysis step. OPSEC measures are usually implemented to mitigate risk in priority order (highest risk to least) minimizing vulnerabilities having the most significant adverse impact upon the activity or organization.

OPSEC measures implemented as a result of the OPSEC process are documented in either an organization or program OPSEC plan and are in accordance with the strategies and guidance provided by the organizational OPSEC program.

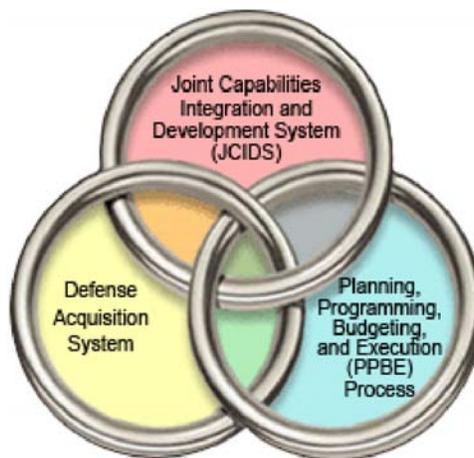
As an aid in conducting OPSEC analysis and assessments the IOSS, in partnership with the Office of the Undersecretary of Defense (Intelligence) and a working group comprised of subject matter experts from throughout the DoD, have developed an automated tool for OPSEC practitioners know as OSCAR (Operations Security Collaboration ARchitecture).

OSCAR provides an automated assessment and analysis tool that compliments local OPSEC expertise. OSCAR is agile enough to meet unique user requirements, enable the user to simulate alternative OPSEC scenarios and contains a customizable reporting tool for presenting the outcomes of OPSEC analysis and assessments. An added benefit of OSCAR is the capability it provides the user to locally tailor standard Defense Intelligence Agency global intelligence threat assessments to the specific operations.

Accessing OSCAR requires user access to the SIPRNET. Requests for OSCAR accounts may be submitted via the SIPRNET at <https://owscar/dtic.smil.mil/oscar>.

An expanded list of potential OPSEC measures is provided at www.iooss.gov / Library Resources/ Operations Security Joint Publication 3-13.3, 29 June 2006/ APPENDIX C.

Overview of DoD Acquisition (A Convergence of Systems and Critical Information)



The DoD acquires a varied array of goods and services in order to successfully perform its mission to provide the military forces needed to deter war and protect the security of the United

States of America.⁸ Effectively obtaining these goods and services often requires effective management of a complex acquisition system encompassing the design, engineering, construction, testing, deployment, sustainment, and disposal of weapons or related items acquired under contract.⁹

DoD acquisitions are successfully managed through a triad of systems. The DoD Acquisition Management System (DAMS), the DoD Joint Capabilities Integration and Development System (JCIDS) and the Planning, Programming, Budgeting and Execution Process (PPBE). The JCIDS identifies and validates DoD capability requirements through a document known as the Initial Capabilities Document (ICD), forming the basis for any major systems acquisitions and tying the supporting activities of the DAMS and PPBE to national defense strategic priorities.

The Planning, Programming, Budgeting and Execution Process (PPBE) develops DoD appropriate budget proposals for the research, development and acquisitions to meet the requirements of the ICD. The PPBE also monitors budget execution (expenditure of funds) during the entire system acquisition in accordance with funding approval granted through the legislative process.

The Defense Acquisition Management System (DAMS) seeks out the best materiel acquisition alternatives and strategies for fulfilling the ICD requirements communicated by the JCIDS in accordance with the law (Federal Acquisition Regulation (FAR), Annual Authorization and Appropriation Acts, etc.) and applicable DoD policy (DoDI 5000.1 and DODI 5000.2, etc.). Controlled, but unclassified, information, necessary to successfully manage large acquisitions may provide an adversary with unwanted insight into DoD plans, intentions and capabilities. The result can be costly system redesign, schedule delays, degraded system performance, or worse. The goal of OPSEC is to systematically identify and protect this “critical information” in the acquisition process through integration of proven OPSEC principles and practices.

The DOD Acquisition Management System (DAMS)

The DAMS consists of five discreet phases:

Material Solution Analysis Phase (MSA),

Technology Development Phase (TD),

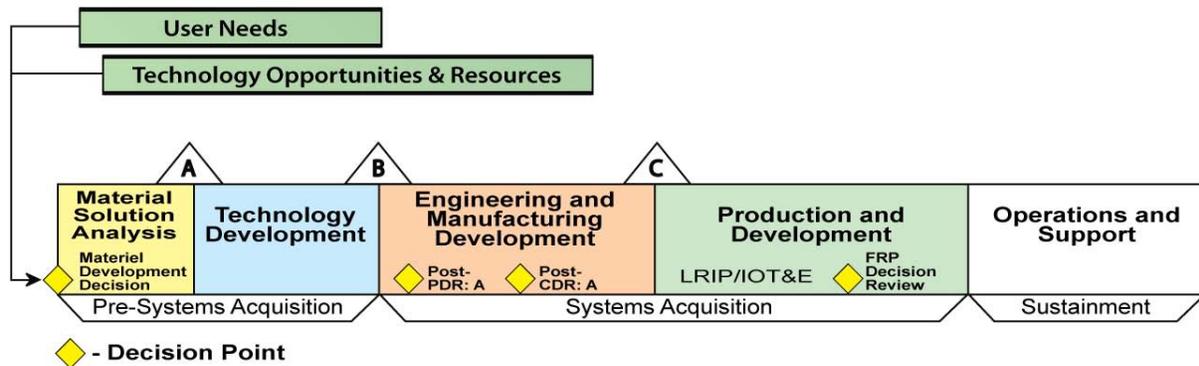
Engineering and Manufacturing Development Phase (EMD),

Production and Deployment Phase (PD)

Operations and Maintenance Phase (OM).

⁸ <http://www.defense.gov/pubs/dod101/>, March 26, 2010.

⁹ Defense Acquisitions: How DOD Acquires Weapon Systems and Recent Efforts to Reform the Process, Congressional Research Service, July 10, 2009, 7-5700



Progression through the acquisition phases is regulated by a series of milestone reviews chaired by a designated Milestone Decision Authority (MDA). Each milestone (A, B and C) provides an opportunity to review acquisition progress and ensure proposed systems acquisitions are meeting JCIDS communicated capabilities requirements.

The formal entry point into the DAMS is the Material Development Decision (MDD) review chaired by the MDA. At the MDD the assigned DoD component presents the ICD, guidance is issued for an Analysis of Alternatives (AoA) Study and funds are identified via the PPBE for MSA phase activities. The MDA may authorize a program to enter at any point in the acquisition system as long as the program meets the standards for that phase of the system.

Pre-Acquisition activities, including fundamental research and development (R&D), are often conducted prior to an official designation of an acquisition program. For example, in FY2010 DoD sponsored basic research to advance technology in cyber-protection, medicine, high performance computing and composite metals which may eventually provide benefit to multiple DoD acquisition programs. R&D is often conducted in partnership with Universities, and amongst Government laboratories without an obvious direct link to a specific acquisition. The absence of this direct link **does not** imply a lack of critical information requiring OPSEC measures.

During the pre-acquisition stage within the DoD, OPSEC must be applied in order to sustain or advance the DoD technological lead in the future battle space.¹⁰ OPSEC practices as prescribed by the R&D organization's resident OPSEC Program are to be incorporated into all pre-acquisition activities. In order to assist Federal Executive Agencies establish a resident OPSEC program, the IOSS offers OPSEC training and awareness support which may be requested <http://www.ioass.gov>.

Material Solution Analysis Phase (MSA)

During the MSA phase alternative materiel solutions for meeting the capabilities described in the ICD are identified, analyzed and documented in an Analysis of Alternatives (AoA) Study.

¹⁰ Department of Defense, Acquisition guidebook, Chapter 8, Section 8.3.1.2, <https://acc.dau.mil/CommunityBrowser.aspx?id=322411&lang=en-US>

The AoA Study assesses critical technologies associated with each proposed materiel solution, including technology maturity, integration risk, manufacturing feasibility, demonstration needs, effectiveness, cost, schedule, concept of operations and overall risk.¹¹

Typical OPSEC concerns during this phase of the DAMS may include; the unauthorized disclosure of the government's interest in a particular technology to meet a perceived operational weakness, the probability a particular technology solution can meet ICD requirements, or unique proposed integration solutions of existing technologies. Much of this information may be inadvertently disclosed by researchers during data collection in support of the AoA Study.

MDA acceptance of the materiel solution recommendation(s) for meeting the expressed capability need in the ICD, and the Technology Development Strategy (TDS) at the milestone A review, mark the end of the MSA phase and entry into the Technology Development Phase (TD). Typically the TDS forms the foundation for the Request For Proposal (RFP) for Technology Development contracts to follow in the TD phase and formally documents the existence of potential critical information.

Technology Development Phase (TD)

The acquisition purpose of the TD phase is the reduction of technological risk and a determination of appropriate technologies which may be integrated into a system in accordance with the approved TDS. The TDS describes how each required technology will be developed. Inherent to most TDSs is a prototype demonstration requiring a close working and/or contract relationship between the government, academia and/or industry.

Additional significant activities that occur during the TD phase include the development of an Initial Product Support Strategy, Preliminary Design Reviews, System Performance Specifications and an Acquisition Strategy for subsequent Engineering and Manufacturing contract(s).

Typical OPSEC concerns during this phase of the DAMS may include; revelation of the geographic locations of logistics depots, unique acquisition strategies that may point to a single vendor, or system performance goals.

MDA acceptance of an Acquisition Strategy (AS) and the Acquisition Program Baseline (APB) at the milestone B review, mark the end of the TD and entry into the Engineering and Manufacturing Development Phase (EMD). The AS forms the foundation for the RFP for Engineering and Manufacturing contracts to follow. The APB sets thresholds and objective

¹¹ http://www.dau.mil/pubscats/PubsCats/13th_Edition

performance parameters for monitoring program success such as cost, schedule, and performance.¹²

Engineering and Manufacturing Development Phase (EMD)

EMD normally initiates an acquisition program and begins at the completion of the milestone B review. The EMD consists of two major subparts: Integrated System Design (ISD) and System Capability and Manufacturing Process Demonstration (SCMPD). The purpose of the EMD phase is to develop and demonstrate a fully integrated system(s) that is affordable, manufacturable and sustainable.

During the ISD subpart systems functionality and interfaces are defined and complete hardware and software detailed designs are generated. The feasibility of the proposed systems design is validated through the successful completion of a Critical Design Review (CDR) ensuring all key performance parameters are met by the final design. Upon successful completion of the CDR, and acceptance of the Post-CDR Assessment by the MDA the ISD subpart concludes and SCMPD begins.

The SCMPD subpart requires the manufacture of production representative articles as a demonstration that the system will operate consistent with the key performance parameters and that production can be supported through the demonstrated manufacturing process(es). Performance is validated and documented through a series of tests to include Developmental Test and Evaluation (DT&E) and Operational Test and Evaluation (OT&E). Information which may require OPSEC protection during the ISD and SCMPD subparts may include test plans, schedules and locations, the results of any tests or vendor production chokepoints that may restrict production capacities.

Once the production representative articles have completed all required testing, and the results documented, the program is ready for the milestone C review by the MDA. It is at this point that the MDA will determine whether to commit to begin low rate production of the system, return it to the EMD phase, or possibly terminate the effort based upon system cost, schedule, and performance to date.

Production and Deployment Phase (PD)

The PD phase normally consists of two subparts, Low Rate Initial Production (LRIP) and Full Rate Production (FRP).

LRIP is intended to demonstrate that systems can be successfully manufactured using the designated manufacturing process(es), the systems function in the operational environment (OT&E), and to demonstrate that higher rate production can be achieved. Upon successful completion of OT&E and a successful Full Rate Production Decision review of the program, the MDA may approve the commencement of Full Rate Production (FRP) in accordance with the

¹² C.B. Cochrane, July 2004, Joint Program Management Handbook, Fort Belvoir, Washington, Dane Publishing, pp 20, ISBN:0160731305

Acquisition Strategy developed for FRP. As with the previous phases of the acquisition process the Acquisition Strategy developed during the LRIP forms the basis for the FRP contracts to follow.

FRP, The second subpart of PD, begins the manufacture of systems to be deployed. This phase overlaps the Operations and Support phase (OS) since early production systems are operated and sustained as FRP is underway and Initial Operational Capability (IOC) is achieved. Information that may require OPSEC protection during this phase may include production capacities, shipping schedules, locations and delivery dates, shortages of critical components or manpower.

Operations and Support Phase (OS)

The OS phase of an acquisition is typically where the military takes ownership of each system providing for any life cycle support in accordance with the Product Support Strategy (PSS) necessary to maintain system readiness to meet operational needs. During this phase Final Operational Capability (FOC) is achieved.

The OS phase of an acquisition typically is the longest phase of an acquisition, concluding upon final disposal of the system at the end of its operational lifecycle. During a systems lifecycle it may be located in remote areas throughout the globe, in less than ideal operational conditions and require multiple vendors to support or maintain system readiness. Each of these requirements may increase the OPSEC risk involved with the system and must be accounted for in OPSEC acquisition planning. For example, if multiple maintenance vendors are necessary, the OPSEC risk due to a HUMINT threat may rise. Logistical data (i.e. supply orders, specific shipping locations, number of systems awaiting repair, etc.), if obtainable by an adversary through open sources, could lead to reduced system performance and/or mission failure.

Additional detailed descriptions of the DoD acquisition system and acquisition resources may be obtained from the Defense Acquisition University website at <https://dap.dau.mil>.

OPSEC Requirements in DoD Contracts

Although many DoD contracting actions are tied directly to a major systems acquisition, many mission critical contracts are not. For example, DoD contracting activities provide support during Pre-Milestone A Research and Development activities and many non-program specific procurements commonly related to facility infrastructure and services. In all cases, OPSEC should be considered early in the contracting process and collaboration between the requiring organization, the OPSEC Program Manager and the contracting activity ensures OPSEC will be effectively applied where required.

Several recent procurement examples point to typical OPSEC concerns involving contract actions. For instance:

A diagram of the perimeter of the building, electrical sources, etc. is a necessary part of an RFP for the procurement of a local building security system. The diagram provided to potential vendors should provide only that information necessary to perform the contracted service. Providing a diagram that reveals superfluous information such as desk numbers, interior walls, seating arrangements throughout the facility may provide an adversary with unintended information about manpower (size and seniority), location of conference rooms and computer systems.

Naming a specific vessel that will be out of service for dry dock repairs and the period of time that the vessel will be unavailable (i.e Request for Dry Dock services for the SS Minnow, a 300 foot ABC Class Fishing Boat. Period of Performance will be five (5) calendar days with a start date on or about February 17, 2010). It may not be necessary to reveal to the public (or an adversary) that a specific vessel will be out of service for a specific time period. Rather than naming the specific vessel, possibly the ship class would be sufficient to allow for service providers to respond to the RFP. Knowing a specific vessel's status, if aggregated with a ship's crew list, may provide an adversary insight into the whereabouts of a targeted crew member during the drydock period.

Publicly posting organization charts, or aggregate listings of acquisition program personnel, to include name, position, phone numbers and email addresses on FEDBIZOPS. Although some points of contact and contact information are necessary to successfully complete the procurement process, aggregated data should either be limited or protected.

Pre Contract Award

Ideally in non-acquisition contract actions, OPSEC requirements should be identified by the requiring organization (Project Lead, etc.). In acquisition programs the OPSEC requirement will be identified by the acquisition program manager and approved by the Milestone Decision Authority (MDA) throughout the acquisition milestone review process.

The requirement for OPSEC measures and the identification of known critical information in need of protection must be clearly stated in the Request for Proposal (RFP) and contract documents. Typically an approved Critical Information List (CIL) and/or OPSEC Plan will be included as attachments to the RFP and referenced within the contract. A DD254 must also be included in all classified contracts, or contracts requiring access to classified information, and may also include specific OPSEC measures the contractor will be required to implement.

In most cases, due to the volume of requests and specialized technical knowledge required to identify the need to protect critical information, the contracting officer will rely upon the judgment of the requiring organization in determining critical information and the necessary OPSEC measures each contract will require.

It is highly recommended that as a part of the RFP contracting activities require submission of a vendor's Corporate OPSEC Program and/or plan(s) as a part of the proposal to be evaluated prior to contract award. Both documents will provide the government insight into the likelihood a vendor will succeed in generating and/or adhering to a Program OPSEC Plan.

Should critical information need to be released to vendors as a part of the RFP process it may be posted to the FeDTeds webpage rather than directly onto FEDBIZOPS.¹³ FeDTeds allows the contracting activity to actively control vendor access to critical and classified information.

The legal requirement for public disclosure of information should not, in and of itself, be permitted to pose an unacceptable OPSEC vulnerability.

Contract Documentation

Whenever a contractor will be expected to implement OPSEC measures, the requirement for such measures will be included in the SoW or a Contract Security Classification Specification (DD254).

If the contractor is required to create an OPSEC Plan the requirement **must** be included within the SoW and with reference to the appropriate Data Item Description (DID) DI-MGMT-80934B referenced in the Contract Data Requirements List (CDRL). As with all DIDs, DI-MGMT-80934B may be tailored by the government to include only that information that is necessary to convey to the government that critical information will be adequately protected.

If the contractor is required to follow the provisions of a pre-existing OPSEC Plan the requirement will be stated in the contract SoW and/or on the DD254. A copy of the plan (or relevant portions thereof) must be included in the RFP so that the contractor is aware of the critical information to be protected and the OPSEC measures expected during contract performance. For example, work that is to be conducted on a military facility may require the contractor to comply with the local OPSEC Plan.

In the event the Government does not require compliance with a tailored written OPSEC plan, the Government may still prescribe specific OPSEC measures as a contract requirement within the SoW or DD254 (ie. annual contractor employee OPSEC awareness briefings, approval of all press releases, shredding waste paper that contains critical information or may be indicators thereof, etc.).

With OPSEC properly required and documented, the Contracting Officer is responsible for selecting and incorporating the appropriate FAR and DFAR clauses into the RFP and contract.

¹³ "What is FedTeDS", <http://www.acquisition.gov/articles/may2007>

A general sampling of possible contract clauses the Contracting Officer may insert in the contract include:

Sample Federal Acquisition Regulation (FAR) Clauses¹⁴

52.204-2 Security Requirements (Aug 1996)

52.225-19 Contractor Personnel in a Designated Operational Area or Supporting a Diplomatic or Consular Mission Outside the United States

Sample Defense Federal Acquisition Regulation Supplement (DFARS) Clauses¹⁵

252.204-7000 Disclosure of Information (Dec 1991)

252.204-7003 Control of Government Personnel Work Product (Apr 1992)

252.204-7005 Oral Attestation of Security Responsibilities (Nov 2001)

252.204-7008 Requirements For Contracts Involving Export-Controlled Items (Jul 2008)

252.223-7007 Safeguarding Sensitive Conventional Arms, Ammunition and Explosives (Sep 1999)

252.225-7040 Contractor Personnel Authorized To Accompany U.S. Armed Forces Deployed Outside The United States (Jul 2009)

252.239-7000 Protection Against Compromising Emanations (Jun 2004)

252.239-7001 Information Assurance Contractor Training and Certification (Jan 2008)

252.239-7016 Telecommunications Security Equipment, Devices, Techniques, and Services (Dec 1991)

252.204-7000 Disclosure of Information (Dec 1991)

DD254 (Contract Security Classification Specification)

Classified contracts and contracts dealing with classified information require the completion of a DD254. The DD254 serves to further alert all parties to the contract requirement for OPSEC measures.

¹⁴ Text for the each FAR clause may be found at <https://www.acquisition.gov/Far/>

¹⁵ Text for each DFARS clause may be found at <http://www.acq.osd.mil/dpap/dars/dfarspgi/current/>

For classified contracts, item 11J of the DD254 is marked, “yes” to alert the reader to the fact that OPSEC requirements exist. If item 11J is marked, “yes” then box 14 of the form should contain local amplifying guidance for the contracting activity and the vendor such as the samples below;

1. *“Compliance with security requirements imposed by documents generated in response to DoD 5200.39, Security, Intelligence, and Counterintelligence Support To Acquisition Program Protection, Sep 10, 97 is required. Compliance with OPSEC measures if imposed by programs supported or by documents generated by [the Contracting Activity or Organization] may be necessary. OPSEC program will be IAW DoD 5205.2, dtd 29 November 1999. Program OPSEC plans shall be coordinated with and approved by [the Contracting Activity] and shall be imposed on subcontractors as appropriate. Program protection measures shall be applied and approved by [the Contracting Activity or Organization] at ALL locations where Critical Information is developed, produced, analyzed, maintained, transported, stored, tested, or used in training.”*
2. *“The contractor shall research, develop and deliver an Operations Security (OPSEC) plan in accordance with the attached DD1423 Contract Data Requirements List (CDRL).”*

In the case of procurements in support of a Special Access Program the following, or similar, text may also be inserted;

1. *“OPSEC requirements may be necessary in the performance of this contract in accordance with individual program requirements and/or the Overprint to the NISPOMSUP. Specific guidance will be provided by [insert SAP OPR].”*

All DD254s, and applicable portions of the SoW referring to OPSEC, shall be provided to the cognizant Defense Security Service (DSS) Field Office and will be used by DSS in support of future industrial security inspections.

Additional information and a comprehensive introduction to the DD254 is available through the Defense Security Service and can be acquired at the following website <https://www.dss.mil>.

Post Contract Award

As with any acquisition or procurement, contract administration is vital to the successful completion of the contract. The Contracting Officer’s Representative (COR) is the key to the verification that required OPSEC measures are adhered to by the contractor during contract performance.¹⁶ **It is the duty of the COR to maintain frequent communications** with the assigned program manager, the contracting officer, local security and the cognizant DSS representative informing each of any noted OPSEC deficiencies during contract performance. The obligation of the COR to notify the contracting officer of any deficiencies noted in either the OPSEC Plan or audits extends throughout the lifetime of the contract.

¹⁶ Based upon the definition of a COR found in the Defense Acquisition University ACQuipedia at <https://acc.dau.mil/CommunityBrowser.aspx?id=290015&lang=en-US>

The COR's duties may include coordination with program and security personnel, as necessary, to grant acceptance of a contractor submitted OPSEC Plan, conduct periodic audits of contractor performance (in coordination with DSS representatives) to ensure the OPSEC Plan is effectively implemented by the contractor and collaboration with DSS representatives prior to DSS annual audits to create an effective OPSEC audit plan.

OPSEC Program, Plans and Assessments

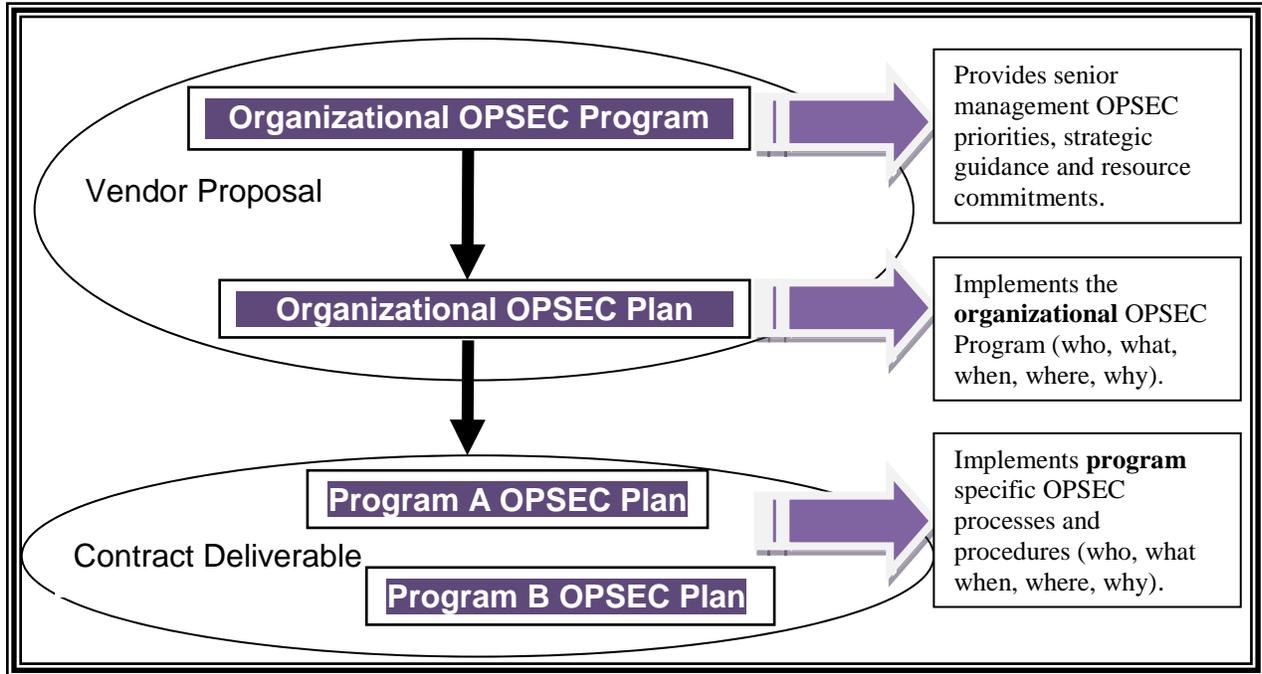
Organization OPSEC Program

An OPSEC Program is, "A comprehensive process incorporating the principles and practices of OPSEC into an organization."¹⁷ Visibly supported by the highest leadership levels it communicates OPSEC as an important component supporting the strategic goals of an organization. Corporate support is imperative as it communicates the importance senior leadership places on OPSEC and provides the means to acquire the necessary resources to make OPSEC planning and implementation a success.

An exemplar organization OPSEC Program ensures a balance between potential loss of critical information and the impact on mission effectiveness, and the attendant cost of such protection.

An organization's OPSEC program may take many written forms, but should always provide a comprehensive description of the organization's OPSEC policy and resources assigned to successfully implement the OPSEC program. Close coordination with traditional security activities is imperative.

¹⁷ Department of Defense Directive Number 5205.02, page 8, dated March 6, 2006.



OPSEC Programs and Plans Relational Diagram

As a part of any contract effort it is highly recommended that a description of the vendor's (organization's) applicable OPSEC program, OPSEC plan(s) and/or OPSEC assessments be a mandatory requirement of all vendor proposals. Required OPSEC program descriptions, plans and assessments should be formally evaluated by the government contracting activity prior to contract award.

Evaluating the offeror's Organization OPSEC Program, Plan or Assessment as a part of the proposal evaluation demonstrates the vendor's corporate commitment to OPSEC practices, substantiates corporate resources and may yield insight into projected vendor costs for OPSEC implementation.

Organization OPSEC Plan

OPSEC Plans are living documents that are used to implement appropriate OPSEC countermeasures given the mission, assessed risk, and resources available to the unit [organization].¹⁸ In an organizational setting the main objective is to add definition and guidance for implementation of procedures and OPSEC measures employed during daily operations of the organization. Senior leadership endorsement of the Organizational OPSEC Plan is tantamount to OPSEC success!

¹⁸ Department of Defense Manual 5205.02-M, page 37, dated November 3, 2008.

The plan documents OPSEC measures, processes and assigns corporate responsibility for the conduct of the OPSEC activities within the organization. It is important to recognize that unanticipated activities and contingencies will arise during the lifecycle of any acquisition. Therefore, all OPSEC plans require periodic review (i.e. OPSEC Assessments or Surveys) and revision based upon changes in the operating parameters (i.e. newly identified critical information, a change in personnel, etc.) or the environment (i.e. a new threat or vulnerability emerges).

Additional guidance for the creation of OPSEC Plans is available at www.iooss.gov / Library Resources/ Operations Security Joint Publication 3-13.3, 29 June 2006/ APPENDIX D & E.

Program OPSEC Plan

A program OPSEC plan is subordinate to the organizational OPSEC plan and addresses similar OPSEC activities within the context of a specific program, contract or acquisition.

An initial OPSEC Assessment is the first step towards creation of any OPSEC Plan. The assessment validates the detailed vulnerabilities in need of OPSEC measures beyond those provided in the Organizational OPSEC Plan (if an Organizational OPSEC Plan exists).

If an OPSEC Plan is a requirement of a government contract, the plan may be either a contract deliverable (written by the contractor) or be provided, in whole or part, to the contractor by the government.

Developing an effective OPSEC plan for an acquisition/contract is contingent upon the author (either Government or contractor) receiving guidance from the sponsoring Government organization or contracting activity. Typical guidance should include identification of critical information in need of protection and the identification of potential adversaries and their intelligence collection capabilities. It is the responsibility of the OPSEC plan author to be well versed in the organization's OPSEC program and plans prior to writing the acquisition/contract program plan.

In the case of a contractor authored program OPSEC Plan that is not required as a part of the original proposal submission, the contractor will submit the plan for Government acceptance in accordance with direction received from the Government contracting activity. Typically Government contracts requiring a contractor generated OPSEC Plan will alert all parties of the need for such a plan through the Contract Security Classification Specification (form DD254 for contracts involving classified information) and/or the Statement of Work. In either case, The the CDRL and the OPSEC Plan DID (DI-MGMT-80934B) will provide the schedule for delivery of the plan and the format for the plan respectively.

If a formal OPSEC Plan is required by the government, the government must be prepared to fund for the creation of a program specific plan and any program specific OPSEC measures adopted in accordance with contract specific terms and conditions.

Additional guidance and discussion of OPSEC Plan(s) contents may be found at www.ioss.gov / Library Resources/ Operations Security Joint Publication 3-13.3, 29 June 2006/ APPENDIX E.

OPSEC Assessments

The effectiveness of OPSEC measures must be evaluated periodically. There are two distinct types of evaluation; the OPSEC Assessment and the OPSEC Survey.

An OPSEC Assessment is,
“A thorough evaluation of the effectiveness of [an organization’s] implementation of OPSEC methodology, resources, and tools.... [and can be] used at the program level to determine whether or not a program is a viable candidate for an OPSEC Survey.”
[<http://www.ioss.gov/glossary.html>]

An OPSEC Survey is,
“...a detailed analysis of all activities associated with a specific operation, project or program in order to determine what exploitable evidence of classified or sensitive activity could be acquired in light of the known collection capabilities of potential adversaries.”
[<http://www.ioss.gov/glossary.html>]

An OPSEC Assessment is a limited, **internal review** of an existing OPSEC Program, or aspect of the program by a small team of knowledgeable OPSEC professionals. In the event no OPSEC program exists prior to the assessment, the assessment provides an analysis of vulnerabilities and may point to the need for an OPSEC program. The primary thrust of an OPSEC Assessment is the answer to the following question, “How well is the organization implementing the current OPSEC Program/Plan?”

OPSEC Assessments are fact-finding activities intended to identify OPSEC vulnerabilities. They are not intended to be punitive or assign blame, and therefore should not be conducted as formal investigations or in an interrogative manner. The positive cooperation of the resident staff and operational experts is key to a successful OPSEC Assessment.

Preparation time for OPSEC Assessments is usually abbreviated and although a formal report may be generated, a memorandum or briefing for leadership may also be acceptable. If an OPSEC Assessment is conducted in response to a Government RFP or contract, format and content guidance must be derived from the appropriate requirements document. Any organization conducting an OPSEC Assessment should expect that the results of the assessment will be protected as proprietary or confidential information and will not be shared outside of the organization or formal acquisition channels (whichever may be applicable).

At a minimum, OPSEC Assessments should be conducted annually, however OPSEC Assessments may be conducted whenever a new need (possibly a new acquisition program) for OPSEC measures arises or a significant change in the threat environment is noted.

Use of the OSCAR automated OPSEC Assessment and Analysis Tool meets all Department of Defense requirements to conduct annual OPSEC Assessments.

Accessing OSCAR requires user access to the SIPRNET. Requests for OSCAR accounts may be submitted via the SIPRNET at <https://owscar/dtic.smil.mil/oscar>.

A typical OPEC Survey involves a thorough examination of an operation or activity to determine if adequate protection from adversary intelligence exploitation exists from the perspective of the adversary. An OPSEC survey will routinely involve a team of OPSEC experts from **outside** of the organization as well as functional experts from within who are familiar with organization operations (communications specialists, logisticians, physical security, acquisition program managers, etc.). OPSEC Surveys are more in depth OPSEC studies and are not routinely conducted on an annual basis. A formal report, in/out-briefings of leadership, including suggestions for correcting problem areas are all part of an OPSEC Survey. OPSEC Surveys are generally beyond the scope of this guidance and general guidance and assistance in the conduct of OPSEC Surveys may be requested from the IOSS website at <https://iad.gov/ioss>.

Conclusion

The nature of effective government acquisition and contracting requires an open exchange of information. In order to support the government's need for goods and services contractors, sub-contractors and suppliers often require details about government operations and intent. Responsively, contractors provide innovative ideas critical to maintaining the United States technological lead in the world arena, especially on the battlefield. Unfortunately, at times, the essential openness of our economic system can lead to compromise of the critical innovations it is intended to promote. Effective minimization of the intersection between openness and compromise is at the heart of OPSEC.

The guidance contained within this document is intended to encourage the acquisition workforce, both government and contractor, to implement good OPSEC practices. Wherever possible the use of, "fill in the blank" style templates has been deliberately avoided so as not to encourage a complacent mentality amongst the practitioner. Successful OPSEC requires active and constant vigilance in order to prevent easily observable activities from telegraphing sensitive intentions and capabilities to the unblinking eye of the adversary.

OPSEC is indeed a mindset and the most critical component to mission and OPSEC success is...

YOU!

Message from the Director, Interagency OPSEC Support Staff

This document is published and distributed by the Interagency OPSEC Support Staff (IOSS) in order to assist U.S. Government departments and agencies and their supporting contractors in establishing and maintaining their OPSEC programs. The information contained herein represents an official formulation, authoritative but not directive, offered by the IOSS to guide the practice of operations security within the Executive Branch.

The IOSS will consider for publication material written on any aspect of operations security (i.e., theoretical, practical, operational, managerial, or historical). If, in the sole opinion of the IOSS, submitted material is acceptable as representing an official formulation to guide the practice of operations security within the Executive Branch, it will be published as such, giving due credit to the author(s). Other material will be considered for publication as monograph, again giving due credit to the author(s).

Manuscripts may be submitted to the IOSS for publication consideration, along with a biographical sketch of the author(s). This sketch should include the current position (Government department/agency, company or military assignment, rank and branch of service of military personnel, mailing address and telephone number). All manuscripts will be acknowledged upon receipt, and a decision to accept or reject for publication will be made as quickly as possible. Manuscripts may be classified or unclassified; however, to reach the widest possible audience, it is preferred that they be unclassified. Responsibility for U.S. Government clearance of articles (when required) and clearance for copyrighted material remains with the contributor. Publication of the manuscript does not imply endorsement by the IOSS or any other U.S. Government department or agency, unless specifically stated, nor does it obligate the U.S. Government to sole source procurement of goods or services. The IOSS does not provide an honorarium for contributors or authors. The IOSS reserves the right to edit all submitted material, and to use all published materials in support of the IOSS mission, including reprinting and distribution of the published material.

Please submit any comments or suggestions for improvement of this publication, and any manuscripts you wish to have considered for publication, to the address below. For additional information concerning IOSS publications, or for handling instructions for any materials classified above SECRET, please contact the IOSS at the telephone the number listed below.

Director
Interagency OPSEC Support Staff
(443) 479-4677
www.iad.gov/ioiss