2013

DEFENSE SECURITY ENTERPRISE STRATEGIC PLAN

Contents

Foreword from the Under Secretary of Defense for Intelligence

The United States and our allies face an evolving, increased, and complex array of threats posed by transnational terrorist groups, international criminal networks, malicious insiders, conventional military forces, and spies acting on the behalf of foreign governments. To combat these and other emerging threats, the Department established the Defense Security Enterprise (DSE), a governance mechanism to implement a federated approach to strategic oversight and advocacy of security capabilities across the Department of Defense (DoD) in support of integrated priority missions. The DSE must have an effective arsenal of enterprise-level security policy and capabilities in order to protect DoD personnel, information, operations, resources, technologies, and facilities.

Security policy, infrastructure and procedure must be operationally relevant, flexible and manage risk. Security practitioners must balance information sharing requirements with the need to protect and foster efficient use of DoD resources. The security profession must evolve to incorporate developmental standards and certifications that better enable personnel performing critical security roles and missions within the Department.

The publication of the initial DSE Strategic Plan serves as a foundation to organize and focus security programs across the Department. It also serves as a guidepost for integrating security strategies throughout the defense community and with our industry partners. Through the partnership and governance process for the DSE, this strategic plan is a framework to explore new initiatives, leverage best practices, and to gain efficiencies across DoD as never before.

I am pleased to endorse the DSE Strategic Plan and look forward to our continued collaboration in implementing this plan to ensure mission success and improve the security of the Department for years to come.

Michael G. Vickers
Under Secretary of Defense for Intelligence

Defense Security Enterprise: 1-Page Strategy

Vision

To seek and enable risk-based mitigation decisions regarding threats and security vulnerabilities related to all DoD assets across the enterprise

Mission

Through partnership and collaboration, integrate and continuously improve security across DoD in support of national security

Goal 1:
Standardize security functions across DoD to achieve synergistic execution and enhance operations

- **Objective**: By May 2013, DoD security costs are quantified
- **Objective**: By Sept 2013, DoD security risks are quantified
- **Objective**: By Dec 2013, a DoD information sharing architecture has achieved initial operating capability
- **Objective**: By May 2014, security cost and risk reduction opportunities are identified, measured, and implemented

Goal 2:
Allocate security resources to demonstrate a return on investment

- **Objective**: By Dec 2013, security has been established as a budgeted DoD program
- **Objective**: By Dec 2014, DoD security ROI is quantified
- **Objective**: By Dec 2014, security ROI improvement opportunities are identified

Goal 3:
Improve individual performance to develop a cadre of highly skilled security professionals

- **Objective**: By Sept 2014, all defense positions that include security as a primary function are identified and documented
- **Objective**: All defense security personnel that are in positions that require certification are certified no later than two years after the position is coded

The Defense Security Enterprise Strategic Framework

Introduction

Security is a mission critical function of the Department of Defense (DoD). Effective security has a direct impact on all DoD missions and capabilities, and on national defense. The absence of an overarching Department-wide security strategy results in inefficiencies and wasted resources, which in turn leaves DoD's mission vulnerable to internal and external threats. The FY12 National Defense Authorization Act also requires DoD to improve information sharing protection and insider threat mitigation for DoD information systems (Section 922).

To reduce deficiencies in security, DoD Directive 5200.43 established the Defense Security Enterprise (DSE) Executive Committee (ExCom)[1]. The ExCom is the senior-level governance body for the strategic administration and policy coordination of the DSE. The ExCom created and tasked the DSE Advisory Group (DSEAG) to plan, coordinate, and prioritize decisions for the ExCom and establish, oversee, and launch project teams. These project teams receive tasks from the DSEAG, research an issue, and recommend a plan of action. The intent of all project teams is to substantively improve the execution of DoD security functions, as defined by DoD Directive 5200.43.

Because of the changing nature of the threats facing the Department and the Nation, the DSEAG will revisit this strategic plan on an annual basis. This will be done to adjust plans and activities to reflect new information and learning. The vision, mission, and goals of the DSE are meant to be enduring elements of the strategy. New objectives and initiatives will be established as the strategy is executed and accomplishments are made. The objectives and initiatives included in this document are starting points for the DSE strategy. They do not encompass all of what can be done, but are what must be achieved first for future successes.

Additionally, as a result of this strategy, changes to current policies may be necessary, and conversely, new policies may require the strategy to be refined. DoD must be prepared to review and adjust policies or the strategy as needed.

This document provides a comprehensive framework that guides the actions of the DSE ExCom and DSEAG as they improve the security posture of DoD. It was collaboratively developed by all members of the DSEAG and represents the best collective thinking from across the Department. For more information on the DSEAG, please see Appendix A.

[1] The DSE is defined in DoD Directive 5200.43 as: "The organizations, infrastructure, and measures (to include policies, processes, procedures, and products) in place to safeguard DoD personnel, information, operations, resources, technologies, and facilities against harm, loss, or hostile acts and influences. This system of systems comprises personnel, physical, industrial, information, operations, and chemical and biological security, as well as SAP security policy, critical program information protection policy, and security training. It addresses, as part of information security, classified information, including sensitive compartmented information, and controlled unclassified information. It aligns with counterintelligence, information assurance, foreign disclosure, security cooperation, technology transfer, export control, cyber security, nuclear physical security, antiterrorism, force protection, and mission assurance policy and is informed by other security related efforts."

Vision

The DSE vision is intended to articulate a desired end state for security. The vision challenges the Department and focuses every level of every component on a single, overarching achievement.

Vision
To seek and enable risk-based mitigation decisions regarding threats and security vulnerabilities related to all DoD assets across the enterprise

The vision breaks down into several important components:

1. ***To seek:*** DSE stakeholders recognize that the threat and risk environments that shape the DSE are highly dynamic and that new threats will continue to emerge.
2. ***Risk-based***: Actions taken to achieve the vision will be based on evidence of threats and vulnerabilities in the conduct of a formal risk assessment.
3. ***Mitigation of threats and security vulnerabilities***: Enterprise initiatives must be focused on improving the DoD security posture. While threat elimination is not possible, vulnerabilities that can be exploited by threat actors will be mitigated to the greatest extent possible.
4. ***Assets across the enterprise***: Assets include people, systems, equipment, facilities and information spread throughout DoD around the world.

Mission

The mission is a simple explanation of what the DSE does. The mission encapsulates all DSE activities, regardless of which component carries them out.

Mission
Through partnership and collaboration, integrate and continuously improve security across DoD in support of national security

The mission does not include oversight of the community, administration of any core security functions, or performance management of other actions not specifically reflected in the mission above. The ExCom's and DSEAG's purpose, in their governance of the DSE, will be to identify and execute specific actions to improve security functions across DoD.

Goals

The DSEAG has defined three overarching goals for the DSE. These goals will serve as the cornerstone of DSE activities and initiatives. Accordingly, they will generate a series of measurable objectives that will allow the Department to measure and manage targeted security improvements across the Enterprise. These three goals are numbered for ease of use and reference; they should not be considered in a prioritized order.

Goal 1:

Standardize security functions across DoD to achieve synergistic execution and enhance operations

There are a myriad of similar security functions being performed in different ways and to differing degrees of success across the Department. The standardization of these functions will create process efficiencies and increasingly seamless integration and synchronization of activities across DoD Components.

Goal 2:

Allocate security resources to demonstrate a return on investment

Goal 3:

Improve individual performance to develop a cadre of highly skilled security professionals

The deliberate and effective allocation of limited DoD resources is a key attribute of a highly functional security enterprise. It is DoD's goal to apply resources to activities that have a demonstrated return on investment (ROI) and positive impact to security.

The effective execution of security functions is critically dependent on the performance of individuals. Therefore, the Department must ensure security professionals meet, and preferably exceed, formally established performance expectations.

Objectives

The mission, vision, and goals provide a high level focus for improving security functions across DoD. The DSEAG also recognizes the need for far more specific targets that can guide tactical activity. Each goal therefore has 18-24 month objectives which are intended to provide the Department with a measurable baseline by which progress can be judged. As the execution of security functions improve and initiatives progress, the DSEAG will revisit the Department's progress against the objectives and adjust milestones as required.

Strategic Goal	Objectives
Standardize security functions across DoD to achieve synergistic execution and enhance operations	By May 2013, DoD security costs are quantified
	By Sept 2013, DoD security risks are quantified
	By Dec 2013, a DoD information sharing architecture has achieved initial operating capability
	By May 2014, security cost and risk reduction opportunities are identified, measured, and implemented
Allocate security resources to demonstrate a return on investment	By Dec 2013, security has been established as a budgeted DoD program
	By Dec 2014, DoD security ROI is quantified
	By Dec 2014, security ROI improvement opportunities are identified
Improve individual performance to develop a cadre of highly skilled professionals	By Sept 2014, all defense positions that include security[2] as a primary function[3] are identified and documented
	All defense security personnel that are in positions that require certification are certified no later than two years after the position is codified

[2] Security is defined in DoD Directive 5200.43 as: "Proactive measures adopted to safeguard personnel, information, operations, resources, technologies, facilities, and foreign relations against harm, loss, or hostile acts and influences."
[3] Primary Duty is defined in DoD Manual 3305.13 as: "Profiled defense security positions that require more than 50 percent of the time performing one or more defined categories of security functional tasks shall be indexed, for certification purposes, as performing defined categories of security functional tasks." This manual will be updated to better align with the recent issuance of DoD Directive 5200.43 as well as the terms and definitions derived from the Federal Interagency Lexicon Working Group.

Initiatives

Through facilitated sessions and one-on-one interviews, the DSEAG has identified initiatives to close gaps between the current state and objectives. The list of initiatives were refined further by analyzing which ones would likely have the most impact and most effectively meet the objectives. The table below documents the team's list of eleven "must do" initiatives. These initiatives provide a foundation upon which other initiatives can be launched. An accompanying timeline is depicted in Appendix C.

"Must do" Initiative	Aligned Objective	Start Date	End Date
Develop framework for cost data collection	By May 2013, DoD security costs are quantified	Aug-12	Dec-12
Collect cost data and determine total costs of DoD security functions	By May 2013, DoD security costs are quantified	Dec-12	May-13
Establish a DoD enterprise methodology to assess and predict security risk	By Sept 2013, DoD security risks are quantified	Aug-12	Dec-12
Quantify most critical risks in order to focus initiatives on priority areas	By Sept 2013, DoD security risks are quantified	Sept-12	Sept-13
Develop and launch the Defense Security Enterprise Architecture	By Dec 2013, a DoD information sharing architecture has achieved initial operating capability	May-12	Dec-13
Develop a DSE-focused Issue Paper for Cost Assessment and Program Evaluation review	By Dec 2013, security has been established as a budgeted DoD program	Aug-12	Dec-12
Refine Issue Paper and insert security into the Oct-Nov 2013 Planning Decision Memorandum for the next Program Objective Memorandum cycle	By Dec 2013, security has been established as a budgeted DoD program	Jan-13	Dec-13
Develop and execute a methodology for identifying and documenting defense security positions	By Sept 2014, all defense positions that include security as a primary function are identified and documented	Aug-12	Dec-13
Codify all relevant positions in the appropriate human resource databases	By Sept 2014, all defense positions that include security as a primary function are identified and documented	Dec-13	Sept-14
Establish minimum competency standards for defense security professionals	All defense security personnel that are in positions that require certification are certified no later than two years after the position is codified	Dec-12	Jan-14
Identify a unifying human capital governance structure	All defense security personnel that are in positions that require certification are certified no later than two years after the position is codified	Aug-12	Mar-13

Summary

Threats and risks to the United States and DoD are difficult to predict and counter. Accordingly, the DSE must be flexible; adapting to threats as they become apparent and before they cause damage. This strategic plan represents the current preferred key goals and objectives for the DSE. It outlines initiatives and objectives that will greatly improve the execution of multiple security functions DoD-wide. This strategic framework will be adapted and modified over time as required.

Appendix A: DSEAG Overview

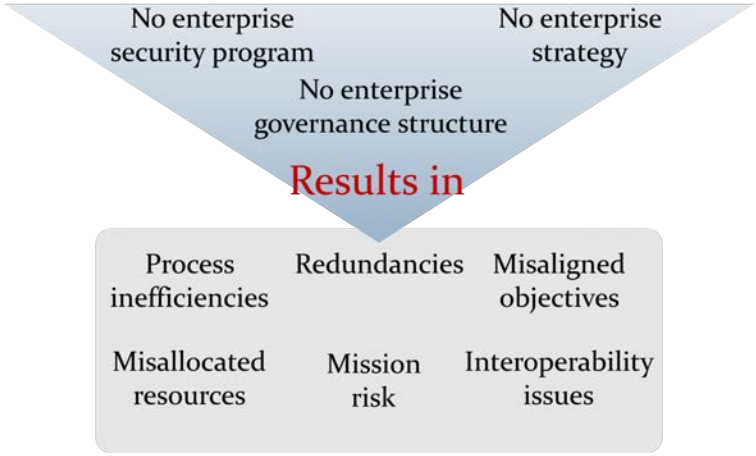
The DSEAG has been tasked by the DSE ExCom to plan, coordinate, and prioritize decisions for the ExCom and establish, oversee, and disband subordinate integrated product teams. These product teams receive tasks from the DSEAG, research an issue, and recommend a plan of action and milestones. The intent of all product teams is to substantively improve DoD security functions.

The DSEAG has met several times to develop and refine a Charter to direct its activities. The Charter includes a definition of the problem they were formed to solve, the scope of activities, and key DSEAG stakeholders.

Problem

The challenges facing the Department's security community are well defined in this and other DoD documents.

The graphic at right depicts the general state of the DoD security enterprise as viewed by the DSEAG. Currently there are many gaps and deficiencies in the execution of the Department's security mission. These deficiencies exhaust valuable resources and introduce unacceptable levels of risk to the missions of DoD Components.



Scope

The security functions within DoD are numerous as well as the threats those security functions seek to mitigate. In order to be effective, the DSE's scope is comprised of security functions contained within DoD. Those functions include: Operations Security, Personnel Security, Physical Security, Special Access Programs, Information Security, Industrial Security (including research and technology protection), and Sensitive Compartmented Information (SCI). For these security functions, the DSE will be known as the primary responsible program. Additionally:

- The DSEAG will be the forum where stakeholders can address cross-functional security problems
- Other critical functions (e.g. information assurance and counterintelligence) will be represented in governance structure and planning for the DSE

The DSE ExCom and DSEAG will build relationships with key allies and partners in order to execute critical goals that have DoD-wide implications.

Stakeholders

The DSEAG consists of core members and ad hoc advisors. The core members are the regular attendees and decision-makers of the DSEAG. The ad hoc advisors are those individuals and groups who are brought in on an as needed basis to address a specific problem or provide unique insight.

Core Members:

- Chair – Deputy Under Secretary of Defense for Intelligence and Security (DUSD(I&S))
- Secretary: Director, Security, Office of the Under Secretary of Defense for Intelligence (OUSD(I))
- Office of the Under Secretary of Defense for Acquisition, Technology & Logistics
- Office of the Under Secretary of Defense for Policy
- Office of the Under Secretary of Defense for Personnel and Readiness
- Office of the Under Secretary of Defense Comptroller
- DoD Chief Information Officer
- Office of the General Counsel, DoD
- Director of Administration and Management
- Joint Chiefs of Staff
- Department of Army
- Department of Navy
- Department of Air Force
- Special Access Program Central Office
- Office of the Under Secretary of Defense for Intelligence / Counterintelligence
- Defense Security Service

Ad Hoc Advisors:

- Office of the Director of National Intelligence
- DoD Non-Intelligence Components
- National Reconnaissance Office
- National Geospatial Agency
- National Security Agency
- Defense Intelligence Agency
- Defense Information Systems Agency
- Combatant Commands

Appendix B: Strategic Framework Gap Analysis

During the strategic planning sessions, DSEAG analyzed gaps between the current situation and future state goals and objectives. These gaps were used to identify root causes of the current situation and tailor initiatives to address these deficiencies. The table below documents the gaps that were identified.

Goal 1:
Standardize security functions across DoD to achieve efficient execution and enhance operations

Objective	Gaps			DSEAG Ideas for Closing Gaps
	Organizational	Policy / Procedures	Processes / Systems	
By May 2013, DoD security costs are quantified	Security is not a DoD budget line, and costs are fragmented	Security is poorly defined and lacks a common lexicon	There is no process or system to compare and audit security costs across the Department	Develop framework for cost data collection
				Collect cost data and determine total costs of DoD security functions
				Ensure standardized security lexicon and vernacular has been documented and integrated across DoD security functions
By September 2013, DoD security risks are quantified	DoD does not have an organizational entity dedicated to security risk management	There is not a formal policy or procedure by which security risks are measured and quantified	There is no standard system or process which measures or quantifies risk	Establish a DoD enterprise methodology to assess and predict security risk
				Design and implement a DoD standard security risk management and mitigation process
				Quantify most critical risks in order to focus initiatives on priority areas
				Standardize use of Enterprise Protection Risk Management
				Improve threat information available in Operations Security Collaboration Architecture (OSCAR)
				Standardize OPSEC assessments and surveys

By December 2013, a DoD information sharing architecture has achieved initial operating capability	No organizational entity for information sharing	No formal policies or procedures for information sharing	There is no enterprise-wide architecture for storing and using data for various security functions	Develop and launch the Defense Security Enterprise Architecture (DSEA)
By May 2014, security costs and risk reduction opportunities are identified, measured and implemented	There are substantial redundancies due to different authorities overseeing different activities in the same process (e.g., personnel security investigations) DoD-wide organizational restructuring launched (e.g., central adjudication facility consolidation), but many efforts have long lead times	Classification procedures and compliance programs are dispersed and decentralized. Policies and procedures for records management need updating/ standardization	There is significant reliance on legacy systems with limited interface capabilities There is no central database to manage contracts Some process and system improvements, but generally at component level (e.g., security clearance process), not DoD-wide	Implement automated records checks in support of continuous evaluation, financial disclosure and other security requirements, in order to decrease PSI costs and potentially eliminate the need for Periodic Reinvestigation products
				Standardize methods of credentialing and continuous evaluation for physical access control of DoD installations and facilities
				Improve record management activities (e.g., classification procedures)
				Centralize and standardize security oversight and compliance programs
				Formalize reciprocity between SCI and Special Access Program communities
				Centralize and standardize foreign travel/contact reporting

Goal 2:
Allocate security resources to demonstrate a return on investment

Objective	Gaps			Potential Actions to Close Gaps
	Organizational	Policy / Procedures	Processes / Systems	
By December 2013, security has been established as a budgeted DoD program	Funding is spread throughout DoD component missions with no centralized decision-making DoD Components often fund only requirements which can be afforded at any given time, rather than planning and securing funds for future requirements		The budgeting and planning process for security is decentralized No centralized system collects and allocates security budget data	Develop a DSE-focused Issue Paper for Cost Assessment and Program Evaluation review Refine Issue Paper and ensure changes are made to insert security into the Oct-Nov 2013 Planning Decision Memorandum for the next Program Objective Memorandum cycle
By December 2014, DoD security ROI is quantified	The lack of an enterprise view of costs and budget means no enterprise view of ROI	There is no standard methodology used to measure ROI	There is no process or system for calculating ROI across security functions	Establish a DoD enterprise methodology for assessing security ROI Design and implement a DoD standard ROI calculation process for security programs Accurately project and program personnel security background investigations requirement across DoD to better inform budgets and resourcing Integrate existing databases to more readily and easily account for current year and out-year investigative requirements Synchronize with acquisition community to better understand program development and related downstream security clearance requirements

Goal 3:
Improve individual performance to develop a cadre of highly skilled security professionals

Objective	Gaps			Potential Actions to Close Gaps
	Organizational	Policy / Procedures	Processes / Systems	
By Sept 2014, all defense positions that include security as a primary function are identified and documented	Reports quantifying the workforce are not inclusive of the entire workforce Primary security functions are sometimes performed by non-security occupation codes Position descriptions with security as a primary duty use inconsistent language for similar security requirements	No Enterprise policy requires collecting and reporting security positions by type: civilian, military, or contractor No policy prohibits non-security occupation codes from performing security as a primary duty	There is no process to identify and report demographics of the entire workforce performing security functions	Collect security position data from across DoD and develop a centralized data repository of all security positions Establish common position description language for similar security requirements Benchmark previous workforce development successes (e.g. information technology / information assurance)
All defense security personnel that are in positions that require certification are certified no later than two years after the position is coded	Certification is largely discretionary; different certifications are needed for different positions	There is no DSE common approach to certification No program in place to vet different certification programs	No process in place to require different certification for different positions	Determine which certification programs meet security standards Require certification for security positions

Appendix C: "Must Do" Initiatives Timeline