

**DoD Strategy
for
Defending Networks, Systems, and Data**



November 13, 2013

**Department of Defense
Chief Information Officer**

DoD Strategy for Defending Networks, Systems, and Data

Introduction

In July 2011, the Department of Defense (DoD) published the DoD Strategy for Operating in Cyberspace (DSOC), stemming from strategic threads outlined in the 2010 Quadrennial Defense Review and 2010 National Security Strategy. The DSOC specifies that cyberspace is an operational domain and DoD should focus its efforts on mission assurance and the preservation of critical operating capabilities. Strategic Initiative 2 of the DSOC (Employ New Defense Operating Concepts to Protect DoD Networks and Systems) called for the implementation of constantly evolving defense operating concepts to achieve DoD's cyberspace mission requirements. This DoD Strategy for Defending Networks, Systems, and Data responds to that requirement as well as other related DSOC initiatives, and identifies strategic imperatives to ensure the protection, integrity, and assurance of DoD cyber¹ assets.

Objectives of this strategy are to:

- Identify strategic imperatives required to focus and transform DoD cybersecurity and cyber defense operations
- Reshape DoD cyber culture, technology, policy, and processes to focus on achieving warfighter missions and needs
- Ensure networks and systems are capable of operating in contested cyber environments
- Position DoD to execute its role in defending the Nation against cyber attacks

Situation

DoD relies heavily on cyberspace to enable its military, intelligence, and business operations, including the movement of personnel and material, and the command and control of the full spectrum of military operations. Exploitation of cyber vulnerabilities could undermine DoD's ability to operate and threaten our national security and economic competitiveness. DoD investments in cybersecurity have improved the security posture of DoD networks, systems, and data by reducing attack surfaces and improving control over information access. Results include enhancements in cybersecurity measures and situational awareness, such as monitoring for intrusions, mitigation of vulnerabilities, improved identity management and authentication, and central collection of incident data. However, the cyber threat is increasing, and adversaries are becoming more skilled, sophisticated, and strategically-minded.

Four Strategic Focus Areas

To meet the challenges expected between now and 2020, transformational changes to DoD's cyber culture, workforce, technology, policy, and processes are required. The results of this strategy will enable DoD to continue to operate effectively in cyberspace, as well as actively defend against adversarial cyber actions. By pursuing the following strategic efforts, DoD will greatly improve its cyber defenses. These initiatives will capitalize on down payments that have been made in each area, yet the current fiscal climate will further challenge the Department to make smart investment choices. These four focus areas and their critical elements are necessary to achieve DoD's cyber mission now and in the future:

¹ For the purposes of this strategy, the terms "cyberspace" and "cyber" are used interchangeably and have the same meaning

DISTRIBUTION A: Approved for public release; distribution is unlimited

- 1) Establish a Resilient Cyber Defense Posture
- 2) Transform Cyber Defense Operations
- 3) Enhance Cyber Situational Awareness
- 4) Assure Survivability against Highly-Sophisticated Cyber Attacks

In these efforts, DoD will work more closely with interagency, private sector, and international partners toward collective cyber defense. Most importantly, the DoD cyberspace workforce will be fully trained, equipped, and prepared for cyber defense of DoD and the Nation.² Although not addressed as a critical element, each focus area will require development of related policy, oversight, and compliance mechanisms. The results of this strategy will produce an achievable end state: *mission dependability in the face of a capable cyber adversary*.

Table 1. Summary of Focus Areas and Associated Critical Elements

Focus Areas	Critical Elements
Establish a Resilient Cyber Defense Posture	<ul style="list-style-type: none">• Architect a Defensible Information Environment• Enhance Security through Cyber Hygiene and Best Practices• Strengthen Data Defenses• Increase Focus on Industrial Control Systems and Embedded Computing• Institutionalize Threat-Based Engineering and Acquisition
Transform Cyber Defense Operations	<ul style="list-style-type: none">• Improve Active Cyber Defense Capabilities• Mitigate All Phases of Cyber Aggression• Ready Forces to Maneuver• Employ Unpredictable Defenses
Enhance Cyber Situational Awareness	<ul style="list-style-type: none">• Improve the Cyber Sensing Infrastructure• Harness the Power of Big Data Analytics• Implement a Multi-Mission Cyber Operational Picture• Increase Information Sharing and Cooperation
Assure Survivability against Highly-Sophisticated Cyber Attacks	<ul style="list-style-type: none">• Assure Survivability of High Priority Mission Areas• Prepare for Success Against Large-Scale Cyber Attacks• Quickly Regenerate Cyber Capabilities

Focus Area 1: Establish a Resilient Cyber Defense Posture

The first strategic imperative, establishing a resilient cyber defense posture, will be achieved through personal security practices, architecture and engineering, and delivery of new capabilities and solutions to address shortfalls in the current DoD Information and Communication Technology (ICT) infrastructure rapidly.³ In addition to the ongoing efforts to provide secure enterprise services, further transformational efforts are required, including secure interoperation with partners. Critical elements include:

² A complementary, comprehensive DoD Cyberspace Workforce Strategy is in development; therefore, specific workforce recommendations are not included in this strategy document except where part of a broader context.

³ ICT is defined in DODI 5200.44, dated 5 November 2012

DISTRIBUTION A: Approved for public release; distribution is unlimited

- **Architect a Defensible Information Environment.** Defending DoD networks against high-tier and advanced threats (e.g., Nation-state adversaries) begins with a defensible architecture that must maintain a high level of operational readiness. Migration to a Joint Information Environment (JIE) will provide a flexible joint warfighting information environment through a shared information technology (IT) infrastructure, enterprise services, coherence with Intelligence Community (IC) capabilities, and a joint security architecture that collectively increases mission effectiveness and enables cyber defense efforts. This JIE security architecture will facilitate technology acquisition and insertion, allow for rapid mitigation response against new threats, increase resilience, and support active cyber defense.
- **Enhance Security through Cyber Hygiene and Best Practices.** Maintaining a defensible network with a high level of operational readiness begins with sound architectural principles that must include cyber hygiene and best practices to maintain the health and resiliency of the network. Cyber hygiene drives network/system health and includes protection, monitoring, maintenance, and design for networks and systems to assure their security and integrity. Ultimately, cyber hygiene strives to create a secure environment that impedes the adversary's ability to gain access, establish a presence and infiltrate deeper in the network, and attack or exfiltrate data in the network. At a basic level, cyber hygiene includes the best practices of hardware and software asset management, along with management of configuration settings and patch level. Increasing understanding of where and how to interrupt the intrusion lifecycle is critical to designing capabilities that harden and defend the cyber enterprise against attack.
- **Strengthen Data Defenses.** Ensuring the confidentiality and integrity of information throughout its lifecycle (i.e., create, transmit, process, and store) is critical to maintaining end-user trust in DoD systems. Robust identities based on public key infrastructure (PKI) and other cryptographic-based technologies are already building a foundation for protecting and sharing information within DoD as well as collaboration with partners. Strong cryptographic-based defenses will become increasingly practical to protect data integrity and confidentiality. Continual modernization and strengthening of current cryptography and key management efforts are required to keep ahead of adversary advances. Finally, DoD will develop and use enhanced metadata tagging and richer access control techniques to improve data access management and discovery.
- **Increase Focus on Industrial Control Systems (ICS) and Embedded Computing.** As ICS and Supervisory Control and Data Acquisition (SCADA) systems are becoming more integrated with IT networks, and embedded IT components are becoming ubiquitous across major weapon systems and tactical communications systems, there is a greater need to secure these systems from remote, external threats both on and off the battlefield.
- **Institutionalize Threat-Based Engineering and Acquisition.** By addressing cyber threats during the full life-cycle of acquisition programs, DoD will design, procure, field, and maintain trustworthy, resilient DoD networks, information systems, and weapon systems. DoD will strengthen requirements, acquisition policies, and directives to ensure that cybersecurity is recognized as essential to achieving capability requirements (e.g., as a key performance parameter) in all DoD acquisitions and that systems security engineering is an early and integral part of all efforts. Engineers, acquisition managers, and logisticians need to integrate cybersecurity strategies more effectively into existing Program Protection Planning, acquisition

oversight processes, and supply chain management. This will ensure that cybersecurity is inherent in the system design, maturing across the lifecycle, and program management decisions are informed by the risks the program is expected to face.

Focus Area 2: Transform Cyber Defense Operations

The second strategic imperative is to shift from reactive cyber defense operations to operations that focus a greater portion of their efforts on adversary activities and intent. As DoD transforms its cyber defense operations, this shift will enable improvements to detect, protect, and respond to the threat's quickly changing cyber tactics. To be successful, the cyber defense workforce will be expert in defensive cyber skills, as well as understand what can be accomplished from an offensive point of view. They will have a dynamic knowledge of the threat's current and projected capabilities, aided by the identification and analysis delivered by intelligence, security, and counterintelligence components. Critical elements include:

- **Improve Active Cyber Defense Capabilities.** “Active cyber defense is DoD’s synchronized real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities. It operates at network speed by sensors, software, and intelligence to detect and stop malicious activity before it can affect DoD networks and systems.”⁴ Active cyber defense is a transformational capability that must be continuously developed and increasingly leveraged in the Department’s cyber defense operations. DoD will refine and evolve its capabilities by leveraging advances in all aspects of cyber operations and integrating national, regional, and organizational cyber defenses into a coherent active cyber defense framework. Additional strategic actions include developing pre-approved options that enable action at network speed, and increasing efforts to detect and identify malicious insider threats, such as increasing the monitoring of high-risk roles.
- **Mitigate All Phases of Cyber Aggression.** Cyber aggression entails multiple lifecycle phases, from reconnaissance and delivery to exploitation and execution; by focusing on each phase of adversary activity, DoD can tailor defensive options to increase our ability to defend against cyber threats. Each of these phases and their associated Tactics, Techniques, and Procedures (TTPs) provides DoD with opportunities to develop and implement layered defenses. Capabilities are required that will divert and slow the adversaries’ efforts, keeping them engaged and wasting their time and effort, thereby allowing DoD to learn from their tactics. This new focus on the attack lifecycle phases will allow DoD to detect and mitigate threats before the adversary can penetrate and establish a foothold, as well as enhance DoD remediation and response activities.
- **Ready Forces to Maneuver.** With the implementation of a defensible Information environment, forces will have improved abilities to shift cyber assets fluidly at network speed when a cyber threat is imminent or underway, such as from a standard operational network to a more secure configuration. This ability to maneuver will result in improved defensive capabilities and increased operational agility. To do this, network operations will require the ability to monitor and change security postures continuously to protect against evolving threat vectors.
- **Employ Unpredictable Defenses.** A static, predictable information environment can allow adversaries to conduct persistent reconnaissance against DoD networks and develop high-probability-of-success tactics. To prevent these advantages, DoD will develop capabilities and

⁴ Department of Defense Strategy for Operating in Cyberspace, July 2011

techniques for non-static security and defenses. These actions will be enabled by the JIE Security Architecture, which will provide an adaptable security framework that allows DoD Information Network (DoDIN) operators and defenders to engineer coordinated changes dynamically across the IT infrastructure, thereby minimizing adversaries' abilities to conduct effective reconnaissance or attack missions.

Focus Area 3: Enhance Cyber Situational Awareness

The third strategic imperative is to enhance cyber situational awareness by significantly improving the sensing infrastructure, focusing on intelligence collection and analysis, and applying advanced correlation and analytic techniques to the resultant Big Data.⁵ Through these efforts, along with a significant increase in information sharing, DoD will develop a deeper understanding of the vulnerabilities facing DoD networks, systems, and data, and their impact on critical missions. Today, cyber forces have difficulty defending mission systems when they cannot “see” what they are defending. Situational awareness empowers local operators to defend their networks and gives mission commanders the awareness needed for maneuverability and response. Critical elements include:

- **Improve the Cyber Sensing Infrastructure.** Threat-based cyber defense requires an improved ability to see and understand cyber activity. A cyber sensing infrastructure consists of sensors that collect information on cyber events and then securely forwards that data to collection points for fusion and analysis. DoD will improve the breadth and depth of the current sensing infrastructure to capture and collect better cyber data in a selective manner. Breadth will encompass more classified and tactical environments, cloud-based services, mobile devices, and other infrastructures upon which DoD depends. Depth will better capture data on anomalous activity that may reveal activities of a malicious insider threat or adversaries who have subverted legitimate user accounts.
- **Harness the Power of Big Data Analytics.** Big Data analytics is the process of examining very large amounts of data to uncover hidden patterns, unknown correlations, and other useful information. Current advances in sharing and fusing cyber threat indicator data will enable the DoD to employ Active Cyber Defense operations, in which increasing amounts of threat indicator data will be available in near-real-time for protection, detection, response, and situational awareness. Similarly, advances in analyzing traffic flow data open new possibilities for detecting anomalous activity including risk assessment outcome-based performance metrics.
- **Implement a Multi-Mission Cyber Operational Picture.** To seize the opportunities afforded by cyber capabilities and mitigate cyber threats, mission commanders need an improved ability to view and understand the cyber environment in a way that correlates with their mission. DoD will develop and evolve a multi-mission cyber operational picture (COP) that provides different user-defined views for network operators (e.g., local view), mission commanders (e.g., regional mission view), strategic threat analysts (e.g., including adversary strategic intent), and supporting intelligence/counterintelligence forces.
- **Increase Information Sharing and Cooperation.** The cyber challenge faced is global in scope, and requires the DoD to collaborate at all levels. Improvements in collaboration and information sharing will substantially increase community synergy across government, industry, international,

⁵ Big Data analytics is the process of examining very large amounts of data to uncover hidden patterns, unknown correlations, and other useful information

and academic sectors. Safe sharing zones implemented by JIE will allow increased sharing with fewer risks to DoD and its coalition partners' networks as well as provide richer interaction with interagency and private sector organizations as appropriate. Enhancing the Defense Industrial Base (DIB) Cybersecurity and Information Assurance Program through increased collaboration with industry is needed to improve information sharing significantly, which will result in the protection of sensitive DoD unclassified information residing on or transiting DIB information systems.

Focus Area 4: Assure Survivability Against Highly-Sophisticated Cyber Attacks

The fourth and final strategic imperative is to ensure that DoD is well prepared to defend against both sophisticated attacks on high priority mission areas, as well as very large scale attacks on the entire DoD enterprise. Resiliency and regenerative methods, including strong, survivable approaches and architectures, will be employed to provide increased confidence that mission systems are neither compromised nor degraded to the point of unacceptable mission impact. Critical elements include:

- **Assure Survivability of High Priority Mission Areas.** For DoD's highest priority mission areas, DoD will re-establish and implement rigorous cyber defense requirements for current operations and future developments.
- **Prepare for Success Against Large-Scale Cyber Attacks.** Planning for and successfully executing a cyber defense operation in the face of a large scale, full spectrum cyber attack requires a broad set of competencies. DoD will increase its development of capabilities that operate at network speed, which will enable cyber defenders to assess, prioritize, re-allocate, and reconstitute cyber capabilities dynamically. DoD must increase efforts to train and exercise against advanced, realistic threats, including large-scale multi-phased and multi-sourced threats.
- **Quickly Regenerate Cyber Capabilities.** DoD will ensure that it has a process in place for restoring capabilities after a successful cyber attack and for capturing lessons learned as a result of a cyber attack.

Conclusions

Implementing the strategic imperatives described in this strategy will require transformation of DoD cyber workforce, culture, technology, policy, and processes, as well as coordination across all DoD components and mission partners. Implementation plans, with discrete actions and tasks and associated schedules and milestones, must be developed and resourced. Executing these next steps will require:

- A commitment to continued and increased cooperation and collaboration across the cyber community, including the intelligence, counterintelligence, and security partners
- Alignment of cybersecurity and defense strategies, plans, projects, and initiatives across DoD
- A DoD organizational construct that will foster the accomplishment of these objectives

Execution of this strategy will ensure that cyber threats on DoD do not have their intended effects. Additionally, this strategy provides DoD forces confidence in the security of their data and freedom of action in cyberspace. Implementation of this strategy will also position DoD for its role in defending the Nation against existential cyber attacks. By 2020, DoD's information enterprise will look dramatically different from today's, with DoD on a path to having the preeminent cyber defense capability.

Appendix A: Acronyms

COP	Cyber Operational Picture
DIB	Defense Industrial Base
DoD	Department of Defense
DoDIN	DoD Information Network
DSOC	DoD Strategy for Operating in Cyberspace
IC	Intelligence Community
ICS	Industrial Control Systems
ICT	Information and Communication Technology
IT	Information Technology
JIE	Joint Information Environment
PKI	Public Key Infrastructure
SCADA	Supervisory Control and Data Acquisition
TTP	Tactics, Techniques, and Procedures