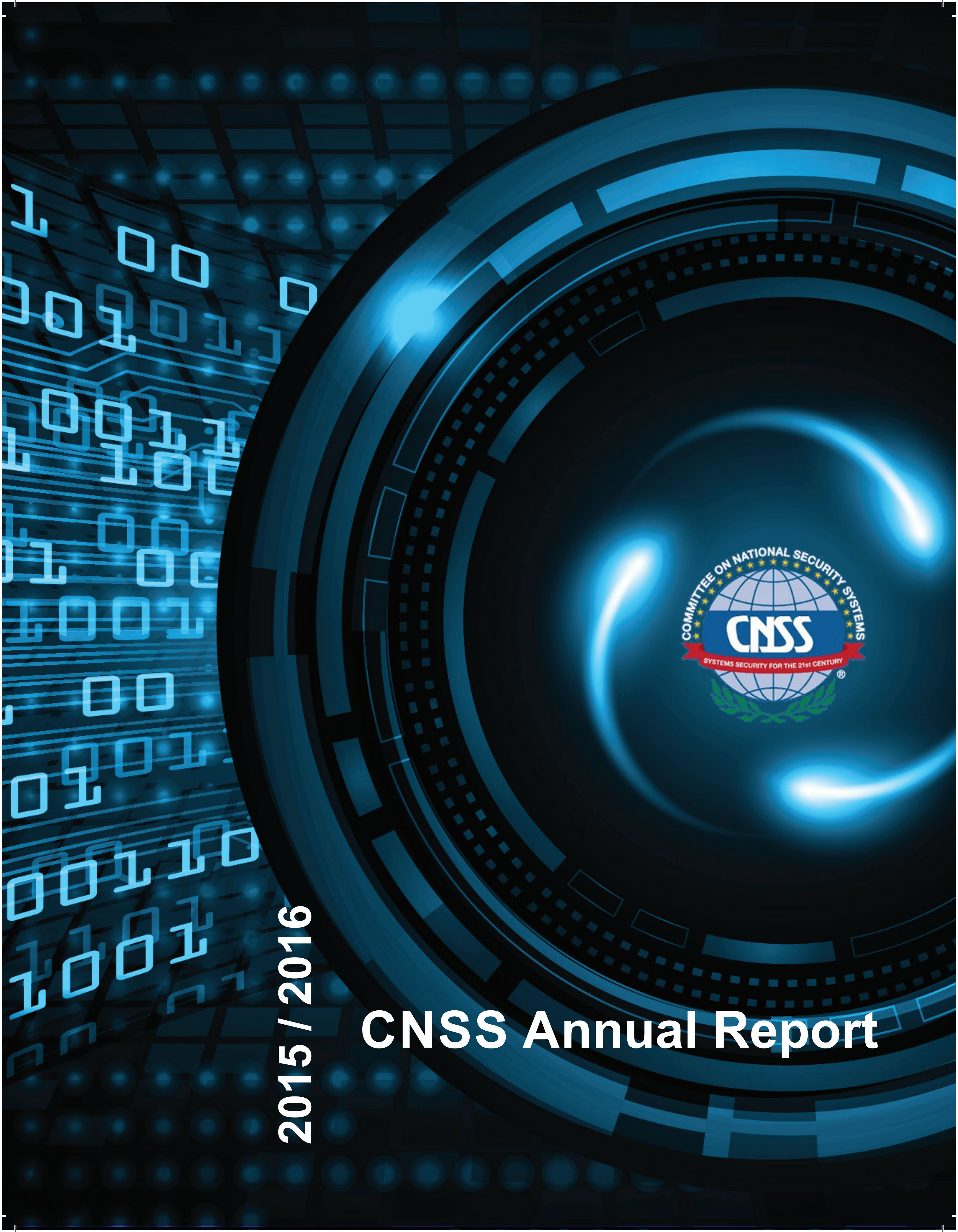


COMMITTEE ON NATIONAL SECURITY SYSTEMS

CNSS

SYSTEMS SECURITY FOR THE 21st CENTURY

2015 / 2016

CNSS Annual Report

DEPARTMENT OF JUSTICE FEDERAL BUREAU OF INVESTIGATION
FIDELITY BRAVERY INTEGRITY
DEPARTMENT OF THE NAVY UNITED STATES OF AMERICA
DEPARTMENT OF TRANSPORTATION UNITED STATES OF AMERICA
JOINT CHIEFS OF STAFF
U.S. DEPARTMENT OF HOMELAND SECURITY
THE DEPARTMENT OF THE TREASURY 1789
DEPARTMENT OF JUSTICE
QUI PRO DOMINA JUSTITIA SEQUITUR
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
OFFICE OF MANAGEMENT AND BUDGET
NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA
DEPARTMENT OF THE AIR FORCE UNITED STATES OF AMERICA
MCMXLVII
DEFENSE INTELLIGENCE AGENCY UNITED STATES OF AMERICA
CENTRAL INTELLIGENCE AGENCY UNITED STATES OF AMERICA
DEPARTMENT OF THE ARMY UNITED STATES OF AMERICA
THIS WE'LL DEFEND
1775
DEPARTMENT OF COMMERCE UNITED STATES OF AMERICA
DEPARTMENT OF STATE UNITED STATES OF AMERICA
GENERAL SERVICES ADMINISTRATION
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE UNITED STATES OF AMERICA
DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA
DEPARTMENT OF THE NAVY UNITED STATES MARINE CORPS
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
DEPARTMENT OF ENERGY UNITED STATES OF AMERICA

Committee on National Security Systems

November 2016

The Committee on National Security Systems (CNSS) serves as a forum for Defense, Intelligence, and Civil users of NSS to deliberate on and promulgate national-level policies, directives, instructions, operational procedures, guidance, and advisories toward the safeguarding of NSS. CNSS works in close partnership with U.S. departments and agencies to develop and implement policy, execute critical programs, and perform essential technical services to strengthen the security of information and communication systems. With diligence and dedication the members of the CNSS Subcommittee, Panels, Working Groups and their subject matter experts have produced a CNSS library that collectively spans an unparalleled spectrum of NSS topics.

As 2015 began, Cybersecurity was among the Nation's most significant national security issues, requiring even more attention as events unfolded throughout 2015 and 2016. President Obama set the tone for U.S. Government efforts to counter Cybersecurity threats when he spoke of increasing efforts to combat the evolving threat of cyber-attacks, identity theft, and deliberate disruption of our Nation's critical infrastructure. CNSS priorities for 2015 and 2016 supported the President's initiative and focused on increasing the level of trust in NSS, increasing protection, and ensuring mission essential functions.

Governance and execution are critical to ensuring that policies and procedures are implemented effectively toward protecting NSS across the interagency. During 2016, CNSS began a strategic thrust to energize hardening and governance of NSS with an initial focus on the Secret Fabric. CNSS is working to establish a Secret Fabric Governance Board and to define mechanisms to track the progress of departments' and agencies' efforts in improving the Cybersecurity posture of their Secret Fabric instances. CNSS is working to improve compliance initiatives through streamlined procedures that reduce the burden of compliance while increasing its effectiveness, and with new metrics and parameters that will increase transparency and enable better measurement of progress.

CNSS, along with its Member departments and agencies, has risen to the challenge of enhancing NSS security in the face of escalating global cyber threats, accelerated by constant evolution of technologies. CNSS has made significant strides in increasing the overall security of the Nation's information systems and networks. We must build on these accomplishments and continue to strengthen NSS and the cyber infrastructure vital to national security.

Sincerely,

Rich A. Hale

Richard Hale
Acting Chair
Committee on National Security Systems

Michael Johnson
Co-Chair
Committee on National Security Systems

Committee on National Security Systems

November 2016

Supporting the work of the CNSS Subcommittee, the CNSS Architecture, Safeguarding, and Operations Policy Panels have continued to provide essential direction and coordination within the CNSS community to address the security challenges facing the Nation. During 2015-2016, the Panels have continued to streamline policy guidance to address threats to NSS and champion significant compliance goals set down in the CNSS Plan of Action and Milestones. In their collaboration with subject matter experts from across the CNSS community, Panels continue to bring cutting-edge developments, innovations, and recommendations together within the working groups by improving efficiency and effectiveness of tasks in development by the CNSS.

The Architecture Panel concentrated efforts on developing an expanded revision of CNSSP 21 dealing with Enterprise Architecture Frameworks to identify the capabilities and standards from which the development and integration of Enterprise Architectures (EAs) shall be designed, and to focus on building architecture frameworks based on the CNSS Enterprise Security Framework and a common set of CNSSI 1253 controls. CNSSP 25 was updated to provide a secure, interoperable mechanism for users to securely authenticate access requests across Secret Fabric Networks. A significant stride was made in 2015 with the publication of CNSSP 7 which provides guidance on the use of commercial solutions to protect NSS and the classified information they contain. TEMPEST specialists developed CNSSI 7003 which established standards for the installation and inspection of Protected Distribution Systems (PDS).

The Safeguarding Panel engaged in the development of guidance regarding the Privacy Overlay designed to protect Personally Identifiable Information (PII) along with improvement of the Risk Management Framework (RMF) across the Enterprise. CNSSI 1254 dealt with assuring reciprocity among CNSS departments and agencies by making appropriate evidence available to all concerned parties. Further revisions to CNSSP 22 took place in 2015 in order to accommodate additional endorsements of RMF standards for NSS and the long awaited update of the CNSSI 4009 CNSS Glossary reduced the potential for misunderstanding among departments and agencies, diminishing confusion that would pose a risk to NSS.

Early in 2015, the Operations Policy Panel established a team to revise CNSSI 1010 with the goal of identifying a centralized reporting center for Secret Fabric incident reports and analysis. The Panel worked to leverage the DoD's insight and knowledge to enhance prioritized capability decisions and enable dependable mission execution on the Unclassified and Secret Fabric. The Compliance and Effectiveness Working Group continued investigating improvements in tracking compliance and evaluating effectiveness of CNSS issuances.

The CNSS Panels and Working Groups under the CNSS Subcommittee have made significant strides to increase the overall security of NSS. They must build on this progress and continue to enhance needed partnerships to achieve success in an increasingly connected and complex environment.

Sincerely,

Daniel Dister Tri-Chair CNSS	Peter Duspiva Tri-Chair CNSS	Kevin Dulany Tri-Chair CNSS

MEDIA
-SHOW BUSINESS
-NETWORK
-INTERNET
-LIVE CHAT
-MEDIA
-PHOTOS
-VIDEOS
-MUSIC
-SHOW BUSINESS
-NETWORK
-MUSIC
-CINEMA
-BUSINESS/FINANCE
-WORLD NEWS
-CULTURE
-ECONOMIC
-FINANCE
-BUSINESS
-MEDIA
-PEOPLE
-CREATIVE
-TUTORIALS
-INVESTMENT
-NETWORKING
-VIDEO
-MUSIC
-SHOW BUSINESS
-NETWORK
-BUSINESS/FINANCE
-WORLD NEWS
STRATEGY
PLAN
INVESTMENT
INCOME
MONEY
-PEOPLE
-FORUMS
-MAIL
-SHOP
-BUY
-SALE
FINANCE
WORLD
1010110110101010110

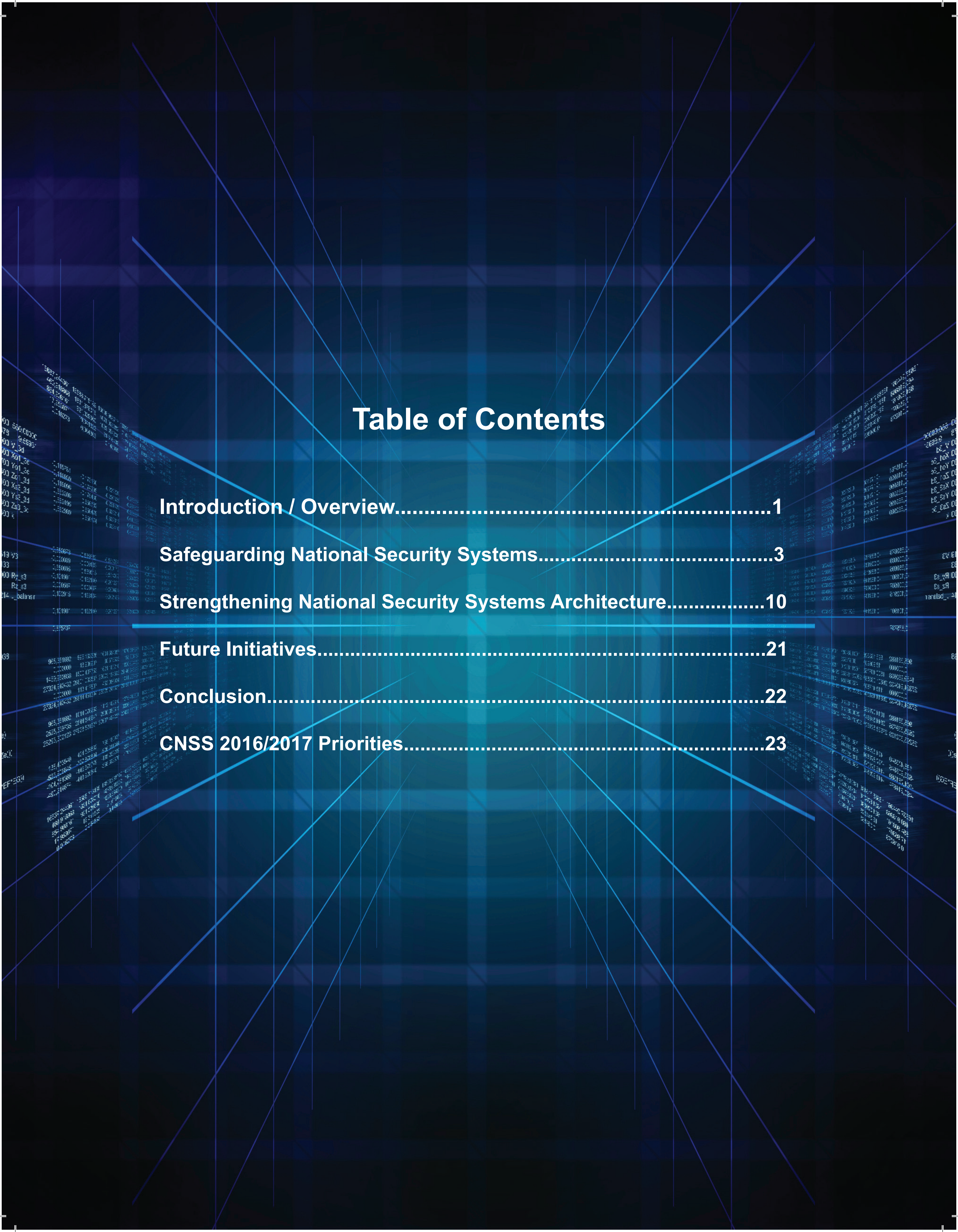


Table of Contents

Introduction / Overview

America's Civil Servants, military personnel, and government contractors rely on National Security Systems (NSS) to accomplish critical missions across the Defense, Intelligence, and Civil departments and agencies of the Federal Government. However, growing numbers of nefarious actors around the globe seek to exploit our Nation's NSS for their own gain—or in the service of our adversaries. To safeguard NSS from technical exploitation, the CNSS serves as a forum for Defense, Intelligence, and Civil users of NSS to develop, coordinate, and issue national-level policies, directives, instructions, operational procedures, guidance, and advisories. The library of CNSS issuances is the result of detailed threat assessments and vulnerability analyses, as well as thousands of hours of painstaking problem solving efforts conducted by subject matter experts whose collective proficiency spans the entire spectrum of Information Assurance and Cybersecurity. These dedicated affiliates hail from the 21 Member and 14 Observer departments and agencies from across the U.S. Government (USG) that collectively form the CNSS.

Our Nation's legacy of interdepartmental collaboration to assure system security can trace its roots to the founding of the U.S. Communications Security (COMSEC) Board in 1953. Nearly four decades of technological advances highlighted the need to expand the focus to accommodate computer system security requirements, resulting (in the 1990) publication of National Security Directive (NSD) 42, *National Policy for the Security of National Security Telecommunications and Information Systems*. NSD 42 established the National Security Telecommunications and Information Systems Security Committee (NSTISSC), which was recast as CNSS in 2001 by Executive Order 13231, *Critical Infrastructure Protection in the Information Age*. Today, CNSS is entrusted with safeguarding the computer systems that host national security information for Federal departments and agencies. The men and women who contribute to accomplishing this mission are dedicated to countering the complex and dynamic threats facing our NSS.

Overview of 2015/2016

Cybersecurity is one of the Nation's most significant national security concerns with an ever growing urgency as events unfold daily that warrant greater protection and safeguards. In his State of the Union address on 20 January 2015, President Obama set the tone for U.S. Government efforts to counter Cybersecurity threats: "We're looking beyond the issues that have consumed us in the past to shape the coming century. No foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets, or invade the privacy of American families, especially our kids. So we are making sure our government integrates intelligence to combat cyber threats, just as we have done to combat terrorism. And tonight, I urge this Congress to finally pass the legislation we need to better meet the evolving threat of cyber attacks, combat identity theft, and protect our children's information. This should be a bipartisan effort. If we don't act, we'll leave our nation and our economy vulnerable."

The White House sponsored several initiatives to improve the Nation's Cybersecurity. For instance, on 13 February 2015 President Obama signed Executive Order 13691, *Promoting Private Sector Cybersecurity Information Sharing*, which is designed to encourage collaboration between corporations and the Federal government on matters of Cybersecurity. On 01 April 2015, the President signed Executive Order 13694, *Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities*, which makes it possible for the government to penalize foreign individuals who engage in cyber attacks that threaten the U.S. economy or National security.

By June 2015, the breach of Office of Personnel Management (OPM) systems made the Nation's Cybersecurity personally relevant to the millions of Americans whose information had been compromised. The OPM—in collaboration with experts from the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI)—responded with investigations and initiatives to prevent any further loss.

Throughout 2015/2016, CNSS rose to the challenge of enhancing NSS security in the face of the increasing severity of global cyber threats, spurred on by the accelerating evolution of technologies. In addition to pursuing ongoing efforts with a renewed sense of urgency, CNSS expanded its analyses of threats and gaps, and refined processes for managing risks. As a result, CNSS has focused on implementing "lessons learned" whenever possible, and spearheading several new initiatives to address the identified gaps. This multi-faceted approach will help assure that the Federal Government stays ahead of the adversaries who seek to harm the U.S. by exploiting our NSS.

Safeguarding National Security Systems

CNSS activities and issuance development in areas such as information system security, risk management standardization, protection of space systems, insider threat, classified information spillage, supply chain risk, standardized security categorization and controls for NSS, and information system authorization provide mechanisms for departments and agencies to safeguard NSS.

Streamlining CNSS Policy Development and Security Control Refinements

Previously, CNSS established new techniques to streamline the development, review, and approval of issuances. Among the most significant innovations in 2014 was the Analysis Paper process, which ensures that all CNSS efforts are purposeful and well-considered before resources are expended. Throughout 2015, CNSS strove to finalize ongoing issuance development efforts and initiate new policy development tasks in response to threat assessments and identified gaps. As CNSS working group members and Panel Co-Chairs implemented the Analysis Paper process, their experiences and lessons learned inspired them to recommend further refinements to CNSS issuance development and review procedures, including:

- Addition of an initial review to expedite proper handling of security controls and control-related topics. Requirements being recommended for publication could either affect the current security control baselines established in CNSSI 1253, *Security Categorization and Control Seclection for National Security Systems*, or be implemented in the form of a security control available in NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*.
- Establishing an initial review of all Analysis Papers by a team of experts who specialize in security controls and CNSSI 1253 baselines and overlays. This review assures that security controls will be addressed appropriately during issuance development, thereby preventing costly delays later in the issuance review and voting process.
- The Analysis Paper review team maintains an open invitation to any CNSS working group considering any recommendations that could affect NIST security controls, CNSS baselines, or overlays.

New Overlay Development: Safeguarding Personal Information in NSS

During 2015, CNSS developed and published one new overlay to the security control baselines for NSS, the Privacy Overlay, Attachment 6 to Appendix F of CNSSD 1253. CNSS security control specialists designed this overlay to protect PII that is present in NSS, regardless of whether the owning department or agency maintains the PII as part of a system of records.

Examples of PII include Protected Health Information (PHI), Social Security Numbers, passport numbers, driver's license numbers, and biometrics (such as fingerprints, voice prints, and facial images) that can be used to uniquely identify individuals. PII can also include data elements that, when combined with other data, can be used to compromise a person's identity—such as zip codes, birth dates, gender, credit card numbers, and bank account numbers. CNSS approved the development of this overlay in order to manage the potential risks that arise when departments and agencies must process or maintain PII. The Privacy Overlay—which was approved in April 2015—is designed to safeguard the PII of the Federal workforce members who serve our Nation in CNSS departments and agencies.

The Privacy Overlay identifies the security and privacy control specifications that are required to protect PII and reduce privacy risks to individuals throughout the information lifecycle. Based on the Fair Information Practice Principles and Federal privacy requirements, these specifications provide a consistent approach within existing NIST and CNSS policies for departments and agencies to implement the appropriate administrative, technical, and physical safeguards, as well as the security and privacy controls necessary to protect PII in today's technology-dependent world.

Improving Risk Management Framework (RMF) Execution Across the Enterprise

CNSS specialists are currently reviewing CNSSI 1253, which contains instructions for performing the Categorize and Select steps of the RMF for NSS, to determine whether these instructions can be enhanced to assure that departments and agencies execute these steps with consistency. Standardizing the system categorization and security control selection processes help to establish expectations across the CNSS Enterprise, so departments and agencies can establish network connections and share information with confidence that the NSS at both ends will be safeguarded as intended.

Globalization of the supply chain increases the challenges in effectively protecting the nation's networks and systems from Information and Communications Technology (ICT) infiltration and attack.

A number of new guidance level documents and controls have been developed through international and national partnerships with government and industry participants. Supply Chain Risk Management threats and vulnerabilities continue to pose increasing risk to NSS capabilities. In addition, risks from the relationships and dependencies of national security capabilities on non-NSS need to be addressed. The existing language in CNSSD 505, *Supply Chain Risk Management (SCRM),* is being addressed by CNSS with the establishment in 2015 of the SCRM Working Group. Since the issuance was not shaped by current lessons learned, best practices, and standards in SCRM that have emerged since the initial publication of CNSSD 505 in 2012, the working group will be undertaking an update of the issuance to reflect the current SCRM taxonomy with issues and challenges faced by the community in today's global sourcing environment. CNSSD 505 will distinguish itself from NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, which is focused on Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, high-impact systems, by engaging the CNSS community beyond the NIST standards, and include a more comprehensive and robust CNSS SCRM focus.

CNSS experts identified an opportunity to improve the execution of the next two RMF steps beyond Categorize and Select—that is, Implement and Assess. Accordingly, in addition to the ongoing review of CNSSI 1253, CNSS approved the development of CNSSI 1253A, *Security Control Implementation and Assessment for National Security Systems*. This Instruction, which was in the early draft stage at the end of 2015, will serve as a companion document to CNSSI 1253.

CNSSI 1253A will leverage the framework for developing assessment procedures presented in NIST SP 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems Organizations: Building Effective Assessment Plans*, and will facilitate security control implementation and assessments conducted within an effective RMF. To date, CNSS subject matter experts specializing in Risk Management, Enterprise Audit Management, and Secure Configuration Management have been collaborating to develop the text for this new instruction. Their goal is to document and disseminate the lessons learned and best practices that have been identified while implementing security controls and assessing them on NSS. CNSSI 1253A is likely to improve the security of NSS and increase the efficiency of executing the RMF by sharing information across the CNSS Enterprise efficiently.

Enhancing System Security and Expediting Mission Accomplishment Through Reciprocity

Strengthening the security control baselines and overlays for NSS have made it possible for Authorizing Officials (AOs) to improve each department's and agency's ability to safeguard the systems for which they have granted an Authorization to Operate (ATO) under the RMF. However, Federal Government operations often involve a high degree of interagency collaboration and cooperation, including the sharing of information technology equipment and networks. Since each department and agency implements the RMF independently, situations have arisen in which it was unclear whether one organization would be able to honor another organization's RMF documentation, including the ATO. For instance, an organization can take ownership of systems that have been authorized by another organization, or a system authorized by one organization can be deployed for connection at a site that has been authorized by another. Situations like these have posed the dilemma of attempting to accomplish the mission with minimal delay as well as safeguarding NSS. In other words, requiring new ATOs for each interagency application of a previously authorized system would seriously hinder the mission, but accepting other organizations' ATOs without question could threaten the security of the hosting network.

CNSS experts identified this gap and dedicated a significant number of man-hours during 2015 to develop and propose a workable policy solution, resulting in the draft of a new Instruction—CNSSI 1254, *Risk Management Framework Documentation, Data Element Standards, and Reciprocity Process for National Security Systems*. CNSSI 1254 will expedite reciprocity among CNSS organizations by setting Enterprise-wide standards for RMF documentation and establishing procedures for departments and agencies to share deploying organizations' information with receiving organizations. Equally as important, CNSSI 1254 also establishes procedures for receiving organizations to dispute security authorization packages if they believe the documentation does not meet sufficiency or completeness requirements in accordance with the RMF. These procedures are designed to assure that disputes can be resolved efficiently and effectively at the lowest possible level.

CNSSI 1254 will assure that reciprocity among CNSS departments and agencies will be achieved through transparency by making the appropriate evidence regarding the security posture of systems in question available to concerned parties. This reciprocity will facilitate acceptance of the existing test and assessment results and security authorization packages that are required by the RMF. Applied appropriately, CNSSI 1254 will reduce redundant testing, assessments, documentation, and thereby save the associated costs in time and resources. In essence, CNSSI 1254 will resolve the fundamental dilemma outlined above by enabling CNSS departments and agencies to accomplish the mission efficiently while assuring that NSS are safeguarded effectively.

Expanding Standards for Risk Assessments and Risk Management

With the publication in 2012 of CNSSP 22, *Policy on Information Assurance Risk Management for National Security Systems*, the CNSS formally adopted the Risk Management Framework and required all departments and agencies to follow NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*. In keeping with the ongoing collaborations and decisions of the Joint Task Force Transformation Initiative Interagency Working Group, the 2012 version of CNSSP 22 also mandates adherence to NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST SP 800-53, and NIST SP 800-53A.

By the close of 2014, a team of CNSS specialists had launched an initiative to update CNSSP 22 to reflect the Joint Task Force Transformation Initiative Interagency Working Group's adoption of NIST SP 800-30, *Guide for Conducting Risk Assessments*. NIST SP 800-30 provides guidance for conducting risk assessments of information systems and organizations, amplifying the guidance presented in NIST SP 800-39. However, before the updated CNSSP 22 could reach its anticipated publication date in 2015, the team elected to further revise and expand the draft of CNSSP 22 to accommodate additional endorsements of RMF standards for NSS. This fully updated draft was released for community-wide review by the end of 2015 and was published in mid-2016.

In addition to NIST SP 800-30, the updated CNSSP 22 cites three additional NIST publications as useful for the CNSS community's risk management programs: NIST SP 800-60 Volume I, *Guide for Mapping Information and Types of Information Systems to Security Categories*; NIST SP 800-60 Volume II, *Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*; and NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*. NIST SP 800-137 will assist departments and agencies that are developing an ISCM strategy and implementing an ISCM program.

CNSS specialists are eager to harness the potential benefits of ISCM to increase awareness of threats and vulnerabilities, enhance visibility into organizational assets, and improve the ability to gauge the effectiveness of deployed security controls.

NIST SP 800-60 Volume I addresses the Categorize step of the RMF and offers guidelines that recommend the types of information and information systems that should be included in each category of potential security impact. This guidance will enable departments and agencies to map security impact levels to types of information and information systems with greater consistency across the CNSS Enterprise. The information types include privacy, medical, proprietary, financial, contractor sensitive, trade secret, and investigation. Information system types include categories such as mission critical, mission support, and administrative. Further information regarding security categorization recommendations and rationale is included in NIST SP 800-60 Volume II. These two volumes will enable departments and agencies to achieve greater reciprocity throughout the CNSS community.

Equally as significant, the CNSS team took this opportunity to incorporate CNSSI 1254 into the mandates prescribed by CNSSP 22. As discussed above, CNSSI 1254 implements an integrated standard for data elements within RMF Security Authorization Packages to facilitate reciprocity across the CNSS community. The pending publication of both CNSSI 1254 and the updated CNSSP 22 will represent an order of magnitude improvement in the CNSS community's ability to execute the RMF in a standardized fashion, and to enhance both information sharing and system safeguarding through improved reciprocity.

Establishing a Standard Lexicon Across the CNSS Enterprise

Although CNSSI 1254 and CNSSP 22 will blaze a path towards reciprocity, CNSS Cybersecurity specialists concluded that cultural and experiential differences among CNSS departments and agencies posed significant roadblocks that could complicate the achievement of that desired outcome. In particular, specialists discovered an alarming disparity among departments and agencies in the terminology and semantics used both in everyday parlance and formal documentation, particularly in the constantly-evolving field of Cybersecurity. On a positive note, this disparity was identified as a topic of concern largely as a result of the close collaboration among departments and agencies in CNSS working groups and panels. To ameliorate this concern, CNSS decided to comprehensively revise CNSSI 4009, *Committee on National Security Systems (CNSS) Glossary*.

CNSS specialists and volunteers from across the Enterprise chose to focus on citing authoritative published sources for the definitions of terms, thereby assuring maximum credibility and acceptance of the resulting Glossary. However, the main challenge was to resolve differences between the departments' and agencies' definitions of terms—particularly between the Defense community, Intelligence community, and Civil agencies. By debating the definitions of each term and arriving at commonly accepted definitions, the CNSS specialists who revised CNSSI 4009 established a consistent standard for the terminology used in documentation, policy, and processes in all communities—including the documentation required by CNSSI 1254.

The updated CNSSI 4009 was completed in early 2015 and published in April of that year. This new standard lexicon will significantly reduce the potential for misunderstanding among departments and agencies that otherwise could result in the kind of confusion that poses a risk to NSS security.

In addition to adopting and enforcing the use of the updated CNSSI 4009, CNSS continues to explore innovative methods for vetting emerging Cybersecurity terms and adding them to CNSSI 4009 efficiently, thereby assuring that CNSS organizations will continue to expedite and enhance reciprocity and ensure effective collaboration across the CNSS Enterprise to safeguard NSS, no matter how the technologies and threats evolve.

Assuring Proper Classification Across the CNSS Enterprise

To foster and maintain reciprocity across the CNSS Enterprise, it is important to assure that Original Classification Authorities (OCAs) at each of the departments and agencies use a common standard for classifying and declassifying information. To achieve this objective, a team of CNSS specialists investigated the prospects for updating National Telecommunications and Information Systems Security Instruction (NTISSI) 4002, *Classification Guide for (COMSEC) Information*. NTISSI 4002 includes directions for classifying COMSEC equipment and materials, as well as information. The team concluded that updating NTISSI 4002 would require a substantial effort due to the significant regulatory, legal, and technological developments that have transpired since 1986, when the document was published.

The team decided that a broader solution was necessary to safeguard systems more completely and to reduce gaps in protection that could result when information is improperly classified and declassified—gaps that the Nation's adversaries could exploit.

Instead of attempting to update NTISSI 4002, the team created a new Instruction to regulate the overarching processes for creating and sharing classification guides. This newly-drafted Instruction, CNSSI 1100, *Consistency and Synchronization During Classification and Declassification of Information Related to Cybersecurity of National Security Systems,* declares that each CNSS department or agency must develop and internally approve its own classification guides based on organizational missions and system requirements.

CNSSI 1100 expedites reciprocity by establishing an Enterprise-wide online repository for storing and sharing these classification guides among departments and agencies. This repository fosters consistency and uniformity in classification and declassification decisions throughout CNSS, since OCAs who are developing or revising their own classification guides will be able to consult current guides that were approved and published by other departments and agencies. CNSSI 1100 encourages reciprocity by directing OCAs to collaborate with the OCAs of other departments and agencies to develop cross-organizational classification guides, when necessary. In addition, the draft Instruction reinforces the processes required for resolving classification challenges among departments and agencies that are entering into cross-organizational agreements, and will synergize with the various initiatives undertaken in 2016 to expand and deepen collaboration and reciprocity across the CNSS Enterprise.

Safeguarding Unmanned Systems That Support NSS

In late 2013, CNSS experts in Space systems—in concert with the National Space Information Systems Security (INFOSEC) Steering Council (NSISC)—began investigating the potential for developing Cybersecurity policies to safeguard unmanned systems.

NSISC includes membership from the National Security Agency, National Reconnaissance Office, Air Force Space and Missile Systems Center, Air Force Space Command, DoD Executive Agent for Space, National Aeronautics and Space Administration, Space and Naval Warfare Systems Command, United States Cyber Command, and United States Strategic Command, among others, many of which are stakeholders in developing and operating unmanned systems.

Their primary concern was that although the use of unmanned systems—in the air, on land, under the sea, and both remotely-piloted and autonomous—had proliferated throughout the previous decade in support of National security missions, no National-level policy had been developed for the implementation of security measures to protect the information residing in or passing through these unmanned systems.

In response to this identified gap, a team of CNSS specialists researched this topic and, in 2014, published a white paper recommending that CNSS should further analyze the Cybersecurity implications of unmanned systems and their operation. Early in 2015, CNSS approved this recommendation and convened a team of CNSS subject matter experts in response.

This team's objectives included conducting a detailed analysis of the characteristics of unmanned systems and sensors that could potentially be translated into Cybersecurity requirements. The team then identified the gaps between the potential Cybersecurity requirements and existing CNSS policy. Early in July 2016, the team submitted a draft of this new issuance—CNSSP 28, *Cybersecurity of Unmanned Systems Used to Support National Security Missions*—for community-wide review and approval.

CNSSP 28 acknowledges that unmanned systems (as well as their supporting infrastructures) require increased assurance and resilience to protect against disruption, degradation, destruction, and adversarial control, and that these protections must safeguard against a variety of risk factors, including environmental, mechanical, and electronic risks, as well as hostile attacks. CNSSP 28 specifies that unmanned systems must undergo the RMF process and obtain the authorization required for all NSS under the RMF. CNSSP 28 also outlines additional considerations that must be addressed due to the special characteristics of unmanned systems and their operating environments. By addressing the gaps identified in the CNSS team's painstaking earlier analyses, CNSSP 28 will provide the Cybersecurity guidance that will help to ensure the protection of our Nation's exponentially-growing fleet of unmanned systems, the safeguarding of the information they contain and process, and ultimately the accomplishment of the national security missions relying on that information and those systems.

Increasing the Focus on Safeguarding the NSS Supply Chain

In April 2015, NIST published NIST SP 800-161, which addresses the risk associated with ICT products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices with the ICT supply chain. NIST SP 800-161 provides guidance for identifying, assessing, and mitigating these ICT supply chain risks.

In accordance with the intent of the Joint Task Force Transformation Initiative Interagency Working Group, CNSS stakeholders reviewed NIST SP 800-161 and determined that NIST SP 800-161 did not offer enough instruction for protecting NSS.

The CNSS team determined that the global supply chain is at the root of the SCRM problem, and that although global supply chain issues cannot be managed from a solely U.S.-perspective, no mechanism currently exists to assure closer collaboration with international allies regarding SCRM. This means that each nation (and often each department and agency) must address the challenge independently. Unfortunately, most departments and agencies do not have adequate SCRM resources to ensure effective implementation of SCRM practices. In addition, the increasing use of commercial components in NSS increases the dependence on external suppliers for sustainment of systems after the components are no longer supported by the original commercial suppliers.

The CNSS team concluded that if these gaps are not addressed, departments and agencies will continue to operate independently with limited SCRM capabilities. To remedy this situation, CNSS launched an effort to revise and expand CNSSD 505, resulting in enhanced interagency collaboration and improved sharing of lessons learned for addressing SCRM.

CNSS departments and agencies will benefit by collaborating not only with government SCRM experts, but also with private-sector experts, research efforts, and academia.This expanded collaboration will increase efficiencies by providing Enterprise standards, best practices, common tools, and shared information for establishing new approaches to SCRM. Increasing the focus on supply chain security represents one of the most far-reaching government-wide undertakings currently in progress for safeguarding NSS.

Strengthening National Security Systems Architecture

CNSS seeks to strengthen NSS Architecture by issuing enhanced safeguarding and technical standards in areas such as enterprise architecture, system security engineering, public key infrastructure, identity and access management architectures, wireless communications, mobile devices, telephony, TEMPEST, and cryptographic modernization.

Strengthening the Standards for Implementing Safeguards in the NSS Architecture

The CNSS Architecture effort includes coordination with organizations across the Federal Government to ensure CNSS architecture efforts are comprehensive and conform to all applicable Federal statutes and Executive Orders and are complementary to other Federal guidance through a liaison with other architectural forums, as necessary, to leverage commonalities and promote consistency across the Federal departments and agencies. Synergy of ideas often serves to enhance the collective efforts of the CNSS community by improving the efficiency and effectiveness of projects that have been approved by CNSS for development. Equally as significant, programs from departments and agencies also inspire parallel efforts in the wider CNSS community. Such is the case with the effort to enhance the Enterprise Architectures for CNSS.

CNSS experts developed and published the current CNSSP 21, *National Information Assurance Policy on Enterprise Architectures for National Security Systems* in 2007.

At that time, each department and agency functioned as an individual enterprise, and each was free to develop its own enterprise architecture for its own systems. Accordingly, CNSSP 21 mandates that all CNSS departments and agencies must employ an enterprise architecture that integrates system security controls, but leaves the minimum controls at the discretion of each individual department and agency. Since that is the case, CNSSP 21 acknowledges that information systems that handle NSI have to operate in conjunction with systems in different departments and agencies whose security needs and architectural requirements vary, and that this disparity impedes the objective of simultaneously achieving the necessary degree of security and the desired degree of information sharing. To address this challenge, CNSSP 21 focused on the Federal Enterprise Architecture (FEA) as the framework to enable CNSS-wide integration, and requires departments and agencies to document their enterprise architectures with the Office of Management and Budget (OMB). The OMB's oversight is intended to ensure that the FEA is being followed, and that there is consistency across departments and agencies.

CNSSP 21 reflects some of the leading architectural concepts of its time. However, since 2007 there has been an increasing emphasis on information sharing and cross-domain capabilities, a growing desire to employ new technologies (especially cloud technologies), and the fielding of new system concepts (such as "system of systems" enterprise concepts). Throughout the emergence of these developments, the Defense, Intelligence, and Civil communities experienced similar challenges in their efforts to share information among their individual departments and agencies while both safeguarding NSS and reducing operational costs.

In response to the developments in architectural technologies and policies throughout the CNSS community such as those represented by the Intelligence Community Information Technology Enterprise (IC ITE) and the Joint Information Environment (JIE), a team of CNSS specialists launched a comprehensive effort to revise CNSSP 21 in 2014-2015, and this effort continues throughout 2016. The CNSS specialists involved in developing CNSSP 21 recognize that the CNSS Enterprise has evolved into a system of systems that is only as strong as its weakest member. Accordingly, the team is developing recommendations for transitioning the entire CNSS community into one architectural enterprise. Doing so would address the shortfalls in the current policy by developing and adopting a single minimum set of acceptable standards that would apply to the entire CNSS community.

As envisioned in the 2016 circulated draft of CNSSP 21, the overarching policy advanced in CNSSP 21 would be implemented and executed by means of additional CNSS issuances that are still under development. One such issuance would establish the CNSS Enterprise Security Framework (CESF), which encompasses four basic Cybersecurity functions: Govern, Protect, Detect, and Respond and Recover. These Cybersecurity functions focus on the capabilities and activities required to provide confidence in cyberspace:

- The Govern portion of the CESF would provide guidance for departments and agencies to manage portfolios and resources, ensure the workforce is informed and engaged, and establish resilience across the enterprise.
- The Protect portion of the CESF would provide guidance for safeguarding the enterprise's physical and logical environment, assets, and data.
- The Detect portion of the CESF would provide guidance for identifying and defending against vulnerabilities, anomalies, and attacks on the physical and logical elements of the enterprise.
- The Respond and Recover portion of the CESF would provide guidance for efficient response mechanisms to address threats and vulnerabilities.

The CESF is intended to be applicable to the full spectrum of departments and agencies, each of which faces different challenges. While CESF would not prescribe one single approach to selecting and implementing capabilities, the framework is arranged in a logical flow, with the governing infrastructure providing a foundation for the enterprise, and the protecting and detecting capabilities working together to safeguard it.

The architectural restructuring envisioned in the current draft of CNSSP 21 reflects the collective expertise of this team, as well as the best practices and lessons learned by those working to restructure the Defense and Intelligence enterprises. Although it will take time to reach community-wide consensus on updating CNSSP 21—and on developing the additional issuance it envisions—the current drafts clearly indicate that CNSS will experience an order of magnitude improvement in both the safeguarding and resilience of the CNSS architecture, as well as in the ability of departments and agencies to network together with security and reciprocity.

Strengthening NSS Architecture Through Identity, Credential, and Access Management Initiatives

The ability to issue and validate strong multi-factor credentials is a cornerstone of the Federal Identity Credential and Access Management (FICAM) initiative. In 2012, the president published the "National Strategy for Information Sharing and Safeguarding," which identified the implementation of FICAM across all security domains as one of its top five priority objectives.

- The National Security Systems (NSS) Public Key Infrastructure (PKI), established in 2009 with the publication of CNSSP 25, *National Policy for Public Key Infrastructure in NSSs*, provides a secure, interoperable mechanism for users to securely authenticate for access to resources across Secret Fabric networks.

- CNSSD 506, *National Directive to Implement Public Key Infrastructure for the Protection of Systems Operating on Secret Level Networks*, published in 2012, was drafted by the NSS PKI Member Governing Body (MGB) in response to Executive Order 13587, which directed structural reforms to provide policies and minimum standards for sharing classified information.

- CNSSD 506 requires all departments and agencies that operate systems on or use the Secret Fabric to implement the NSS PKI and leverage NSS PKI certificates for network logon and for application authentication.

- CNSSI 1300, *Instruction for National Security Systems Public Key Infrastructure X.509 Certificate Policy Under CNSS Policy No. 25*, first published in 2010, 2012, and later in 2014, defines the requirements for the operation of the NSS PKI. The Department of Defense (DoD) and Department of State (DoS) began issuing PKI certificate credentials to their Secret Fabric users shortly after the establishment of the NSS PKI. Recognizing the cost to maintain issuing Certification Authorities (CA), the Office of Management and Budget (OMB) issued a memo in June 2012 directing the establishment of a Common Service Provider (CSP) that would support the issuance of certificates for agencies not already operating their own PKI on the Secret Fabric.

- The DoD accepted the responsibility for operating the CSP under the direction of the multi-agency CSP Governance Board. The NSS CSP PKI, a shared service on the Secret Fabric, became operational in July 2013.

At the beginning of 2015, all of the building blocks were in place for the NSS PKI. As a result, the 2015 focus was on expanding the implementation of the NSS PKI and the ability for Secret Fabric users to obtain and use PKI certificate credentials to authenticate to networks and access resources. Both the DoD and the DoS significantly increased the number of users with hardware token credentials issued under NSS PKI. The FBI, which was already operating a PKI on their network prior to the establishment of the NSS PKI, was issued a cross certificate from the NSS PKI Root CA to permit interoperability while they work to upgrade their infrastructure. There are now nine agencies participating in the CSP, three of whom have provided hardware token credentials to over 80% of their eligible user population.

Incorporating Commercially Available Tools and Technology

One example of a commerically implemented technology is the Secure Mobile Environment Portable Electronic Device (SME PED), a classified mobile device developed by NSA and approved for use on NSS. In recent years, however, U.S. departments and agencies have urgently requested increasingly sophisticated and flexible Cybersecurity solutions that require the use of Commercial-Off-the-Shelf (COTS) products. These requirements extended to classified and sensitive networks, thereby creating the need for a standardized approach for fielding commercial solutions for NSS. Furthermore, departments and agencies have begun to realize benefits from increasing their investments in commercial solutions to protect NSS. The United States Southern Command (USSOUTHCOM) recently saved the DoD $2.6 million by replacing traditional NSA-developed Cybersecurity products with an approved commercial solution.

To meet this rising demand, NSA has invested significant resources to develop commercial solutions that rely on the technique of layering commercial products. The resulting composite commercial solutions can safeguard systems as securely as a developed Cybersecurity product (such as a Controlled Cryptographic Item (CCI) or Cryptographic High Value Product (CHVP)). However, the increasing use of layered commercial products highlighted a significant gap in policy.

The policy in effect as 2015 began governed only NSA-developed Cybersecurity products, not commercial solutions. Once the NSA certifies Cybersecurity products for use, departments and agencies must handle them in accordance with applicable CNSS issuances. For example, the 4000-series of CNSS Instructions governs the use of COMSEC equipment. However, in 2015, CNSS specialists observed that approved commercial solutions were not covered by any CNSS issuances, and the published requirements for developing and fielding NSA Cybersecurity products do not apply to commercial solutions. Moreover, some departments and agencies began to develop local policies for implementing commercial solutions, but without the benefit of an authoritative policy to serve as a standard.

During 2015, CNSS launched an effort to resolve this gap. A team of CNSS specialists developed CNSSP 7, *Policy on the Use of Commercial Solutions to Protect National Security Systems*, which was approved and published in December 2015. CNSSP 7 defines the processes for departments and agencies to obtain NSA approval for using commercial solutions to protect NSS. It provides the requirements for securely implementing a composed commercial solution, and clarifies the responsibilities of the requesting U.S. department or agency for implementing that solution. CNSSP 7 will also serve as a baseline that U.S. departments and agencies can use as a foundation for their own internal policies and processes.

CNSSP 7 will help government departments and agencies reduce the time it takes to build, evaluate, and deploy solutions for safeguarding NSS by employing technologies that are available in the commercial sector. Using commercial solutions will make it possible for departments and agencies to keep pace with technological progress by deploying the latest capabilities in their systems and networks. Experience has also shown that departments and agencies can reduce operational costs by employing commercial solutions.

New Public Cryptographic Standards for Secure Sharing of Information

The Defense, Intelligence, and Civil communities depend on rapid and secure information sharing to protect our Nation, its citizens, and its interests. Modern communications technology can provide the global connectivity required for departments and agencies to collaborate effectively. However, this technology is highly complex, and achieving secure interoperability among information systems can be a challenge. Secure interoperability makes it possible to get the right information to the right users in a timely and secure manner, and achieving secure interoperability to accomplish National-level missions requires cooperation not only among departments and agencies, but also with industry, foreign partners, and international organizations.

To meet this requirement, CNSS published CNSSP 15, *Use of Public Standards for Secure Information Sharing Among National Security Systems*, in October 2016. CNSSP 15 presents a list of publicly-available NIST cryptographic algorithms that have been approved by NSA to protect NSS and the information that they contain or process. CNSSP 15 specifies that information can be shared in an assured, secure, end-to-end manner by using a standard suite of security protocols and these approved cryptographic algorithms. The cryptographic protocols describe how to implement the cryptographic algorithms to achieve interoperability. One benefit of this approach is that protocols and algorithms will be widely available to industry and both U.S. and foreign governments. Another is that the use of standardized protocols is the most efficient way to achieve secure interoperability.

During 2015, the NSA updated the guidance on the public cryptographic algorithms that should be used to protect NSS. CNSS specialists investigated this issue and determined that the public cryptographic algorithms identified in the existing version of CNSSP 15 do not reflect the updated guidance.

Therefore, equipment implementing the current policy might not have NSA approval to protect NSI.

In order to ensure continued NSS security and interoperability, and to avoid wasting the CNSS community's resources on implementing incorrect algorithms, CNSS specialists recommended issuing an Advisory Memorandum to inform departments and agencies of the NSA's updated guidance. In addition, the specialists analyzed the threat to public algorithms posed by adversaries' quantum computing capabilities and identified a set of newly-authorized algorithms that departments and agencies could use in the near term to meet their interoperability requirements. CNSS included this expanded list of authorized algorithms in Advisory Memorandum (AM) Information Assurance (IA) 02-15, *Use of Public Standards for the Secure Sharing of Information Among National Security Systems*, which was released in July 2015.

In the fall of 2015, CNSS specialists developed an updated draft of CNSSP 15 that required departments and agencies to transition to quantum-resistant cryptography. In the interim, CNSS AM IA 02-15, made it possible for departments and agencies to avoid making two major cryptographic transitions in a relatively short time frame. CNSS AM IA 02-15 assured the ability to achieve secure interoperability, safeguard NSS and NSI, and accomplish the mission efficiently and effectively until CNSSP 15 was published in 2016.

Strengthening the Architecture of Protected Distribution Systems

USG departments and agencies—as well as their contractors and vendors—require access to NSI at operating locations worldwide in order to accomplish their mission. One of the most fundamental responsibilities of CNSS is to establish issuances to safeguard NSI against adversarial attempts to intercept or exploit NSS information. The threat level posed by adversaries is determined by the system's AO in consultation with the cognizant Certified TEMPEST Technical Authority (CTTA) and Counterintelligence Coordinating Authority (CICA) responsible for providing Counterintelligence (CI) risk assessments. In locations where this threat is deemed to be high, encryption is required to safeguard NSI that is in transition between systems. However, in locations where the threat of tampering is deemed to be medium or low, encryption of NSI in transition is not necessarily required. In these circumstances, CNSS requires a PDS to safeguard the transmission of unencrypted NSI.

Since the NSI being transmitted through a wire line or optical fiber PDS is unencrypted, the PDS must provide adequate electrical, electromagnetic, and physical safeguards to deter exploitation. For nearly 20 years, the guidance and requirements for the approval and installation of PDS were provided in NSTISSI 7003, *Protected Distribution Systems*, dated 13 December 1996.

To revise NSTISSI 7003, CNSS convened a team of experts—including TEMPEST specialists, who specialize in the investigation, study, and control of unintentional compromising emanations from telecommunications and automated information systems equipment. The team developed CNSSI 7003, *Protected Distribution Systems* (PDS), which was approved and published in September 2015. CNSSI 7003 establishes standards for the installation and inspection of PDS.

CNSSI 7003 also includes guidance to assist the department and agency AOs who must make risk management decisions regarding PDS, since the specific facts unique to each facility tend to increase or decrease the level of risk faced by the PDS.

Emphasis is placed on detecting attempted tampering or penetration, instead of preventing adversarial behavior.

CNSSI 7003 includes instruction regarding the overall security afforded by a PDS, which is the result of a layered approach, incorporating various protection techniques. The criteria for these techniques are based on the threat and assessed risk specific to the planned location of the PDS. In general, this flexibility enables AOs to make determinations that can result in reduced requirements for the installation and maintenance of PDS, which can, in turn, result in cost savings.

Ultimately, CNSSI 7003 enables departments and agencies to protect the NSI that is required for mission success in locations throughout the world—an important step towards assuring not only Cybersecurity, but also our NSS.

Standardizing Incident Reporting and Sharing Lessons Learned Across the Enterprise

CNSS has benefitted from the collaboration of its departments' and agencies' subject matter experts on the broad spectrum of Cybersecurity topics and issues embodied in CNSS policy. In recent years, this collaboration has become increasingly close and productive, as demonstrated by the rising number of successful initiatives designed to standardize procedures, improve the reciprocity among departments and agencies, and enhance their ability to cooperate towards mission accomplishment. Recently, however, CNSS specialists focused on an area in which there has been virtually no substantive collaboration among the entire CNSS community: the response to incidents that threaten the security of a department's or agency's NSS.

CNSS specialists observed that information regarding a cyber incident that occurs in a member of one community (such as the IC) is not being shared with other members of the IC, let alone the entire CNSS community.
The specialists concluded that this gap leaves each department and agency potentially vulnerable to follow-on attacks, even when the first department or agency to be targeted successfully defends against the attacker. The specialists conducted a thorough review of CNSSI 1010, *24x7 Computer Incident Response Capability (CIRC) on National Security Systems*, dated July 2013, and recommended updates. Early in 2015, CNSS established a team to revise CNSSI 1010. The team's goals included identifying a centralized reporting center for Secret Fabric incident reports and analysis, establishing a reporting portal, and standardizing the reporting process by developing a report format and establishing categories and thresholds for cyber incidents and events.

By the end of 2015, the team developed a draft of the updated CNSSI 1010, *Cyber Incident Response*. CNSSI 1010 centralizes Secret Fabric incident reporting, which helps standardize the incident response process across the CNSS community, and improves shared situational awareness across the Secret Fabric. In accordance with the 2014 Federal Information Security Modernization Act (FISMA), the draft CNSSI 1010 requires all departments and agencies that own or operate NSS to establish or subscribe to a 24-hour, seven-days-per-week Cyber Incident Response Capability (CIRC). This capability compliments other Cybersecurity capabilities, and when implemented across all NSS, will help protect and defend networks, provide automated alerts, enhance situational awareness, and preserve evidence of Federal law violations. Additionally, the draft CNSSI 1010 provides guidance on preparing incident response plans and incident reports, obtaining subscriber-based CIRC services, and seeking assistance from the National Security Cyber Assistance Program (NSCAP).

The cyber incident and reportable cyber event categorization appendix to CNSSI 1010 provides a clear cyber incident reporting order of precedence and a specified reporting timeframe. This level of detail is crucial to providing timely incident reporting and provides detailed guidance on not only what to report, but when to report incidents. These measures will assure that the information on NSS is being monitored and protected.

In addition to drafting and reviewing CNSSI 1010, CNSS also identified the Defense community's Joint Incident Management System (JIMS) as the primary incident reporting repository for the Secret Fabric, and established JIMS accounts for members of the Civil and Intelligence communities. CNSS experts created JIMS procedures for reporting incidents and maintaining situational awareness. They also established a capability to triage, analyze, correlate, and fuse incident reports across the Secret Fabric by working with NSA's Information Assurance Directorate for all NSS incidents reported in JIMS. CNSSI 1010 requires NSA to monitor the Secret Fabric Dashboard in JIMS, and to forward a notification to all departments and agencies regarding any anomaly that has been reported. This order of magnitude increase in collaboration and information sharing across the CNSS community will bolster the Enterprise's defenses against current threats and improve the implementation of best practices and lessons learned to safeguard NSS from future threats.

Safeguarding Against Threats Posed by Mobile and Wireless Technologies

The USG has become more reliant on highly capable mobile technologies, which provide users with increasingly sophisticated functionality to support mission needs. The introduction of mobile devices into secure spaces, and the infrastructures to which they connect, pose a threat to classified and sensitive information and systems. Mobile and wireless security measures must be employed to protect mobile devices, and the networks they connect to, from threats and vulnerabilities associated with wireless computing. CNSS develops policies, procedures, guidelines, instructions, and standards as necessary to create national policy specific to mobile and wireless technologies and operational environments that employ mobile devices.

In 2015, in an effort to mitigate the risks associated with the use of mobile technology inside and outside of secure government infrastructures, CNSS began the development of two directives to control the introduction and use of mobile devices in/outside secure spaces:

- CNSSD 510, *Directive on the Use of Mobile Devices Within Secure Spaces*, specifies instructions to control the introduction and use of mobile devices in secure spaces, both domestic and overseas, where NSS may be employed and within government controlled environments where NSI is transmitted, accessed, processed, or stored.

Devices Outside of Secure Spaces, specifies the guidance to control the use of mobile devices outside of government controlled spaces, both domestic and overseas, and to ensure that classified USG mobile devices are protected commensurate with the classification of the information they contain.

Tracking Compliance and Evaluating Effectiveness of CNSS Issuances

The Compliance and Effectiveness Working Group (CEWG) was renamed from its predecessor, the Compliance Assessment Working Group (CAWG) in January 2014, to demonstrate that the CEWG's focus was not on making compliance assessments, but assessing all issuances to extract compliance effectiveness within issuances.

The CEWG measured and managed compliance and effectiveness of CNSS issuances in support of National level goals regarding the security of NSS. The CEWG was also tasked with developing a Compliance and Effectiveness Framework for inclusion in CNSSD 900, *Committee on National Security Systems (CNSS) Governing and Operating Procedures*, developing metrics in support of the Framework, analyzing reported information, and preparing reports for CNSS.

The CNSS Compliance and Effectiveness Dashboard, which was created in January 2014 and updated quarterly with Key Information Sharing and Safeguarding Indicator (KISSI) data, measured how well departments and agencies performed throughout the CNSS community with regards to Safeguarding.

The Dashboard focused on the Five Priority Areas designated by the Senior Information Sharing and Safeguarding Steering Committee (Steering Committee): Insider Threat, Removable Media, Reduce Anonymity, Access Control, and Enterprise Audit. There were concerns about whether the Dashboard data was outdated due to the characteristics of the data being used to respond to KISSI questions and whether new sources of data were required.

Subject matter experts felt that existing KISSI data was inadequate to fully analyze cross-agency compliance. Due to the Congressional inquiry from the House Permanent Select Committee on Intelligence (HPSCI), the value of KISSI to the IC was being assessed. Although Congress was currently using KISSI data, KISSI reporting could be discontinued when a new President is elected into office. New processes will have to be created to keep pace with emerging technologies and new priority focus areas.

Additionally, best practices and challenges from departments and agencies were used to further enhance the compliance and effectiveness structure. One of the best practices revolved around re-educating the CNSS community on how Dashboard scores were determined, which alleviated any misinterpretation on how to measure Dashboard metrics. The metrics developed during the process were used to satisfy CNSS goals, and may be used for annual FISMA reporting requirements.

This was crucial to streamline department and agency reporting because data was collected once, but could be used multipletimes for meeting reporting requirements.

The CEWG continued to evaluate the best way to develop the formal Compliance and Effectiveness Framework in a continuously changing environment. This Framework was initially discussed in September 2014, with the draft of Compliance and (Improvements in) Effectiveness Framework for the CNSS. As the environment has changed, the CEWG brainstormed new ideas, to include actions to be taken for departments and agencies that were not in compliance with CNSS issuances. As it appears that KISSI reporting may cease in the future, this Framework will continuously be reviewed to determine if it is meeting the CEWG's goals in assessing the compliance and effectiveness of CNSS policies. The CNSS Compliance and Effectiveness Worksheet was another tool designed to be used in the Framework and documented requirements contained in issuances so that metrics could be analyzed to determine if the issuance was being utilized properly. The CEWG Charter was also reviewed to determine what changes to make and which data sources to use, as well as the CEWG's role in using those resources. Subject matter experts have been discussing whether the Steering Committee's Five Priorities align with the goals in CNSS issuances, but recommended developing 10 CNSS priority focus areas for the Secret Fabric Governance.

Way Ahead

There is an evolution underway to transform the way compliance and effectiveness of NSS is being managed. The CEWG is part of this reinvigoration process to streamline procedures, without placing additional burdens on departments and agencies. They are transitioning into a rebuilding phase to discuss the current metrics and their goals moving forward. Part of this transition is shifting the focus away from the CNSS Compliance and Effectiveness Dashboard, and to a Secret Fabric Cybersecurity Scorecard similar to the DoD Cybersecurity Scorecard. The Scorecard is part of the DoD's Cybersecurity Discipline Implementation Plan, a document that aims to hold leaders accountable for Cybersecurity and report progress and setbacks. The plan has four Lines of Effort that aim to counter some types of digital exploits potential hackers have used to infiltrate networks, including:

- Strong authentication to obscure adversarial maneuverability within networks.
- Device hardening to reduce internal and external attack vectors.
- Reduction of attack surface to minimize external attack vectors.
- Alignment to cybersecurity/computer network defense service providers to improve detection and response to adversarial action.

The Secret Fabric Cybersecurity Scorecard will be used within CNSS to monitor, track, and manage the security status of NSS by automatically identifying vulnerabilities and providing a more useful tracking mechanism for compliance and effectiveness with CNSS issuances on the Secret Fabric.

The CEWG may also analyze whether Continuous Diagnostics and Mitigation (CDM), or automated data feed, would prove useful in the compliance tracking process. This transition from the CNSS Compliance and Effectiveness Dashboard to an NSS Scorecard shows a shift from primarily focusing on compliance, to making the effectiveness of those security measures a priority.

An effectiveness baseline will be established in order to measure and verify whether security has improved. Another important function in securing NSS is through the implementation of a healthy Cybersecurity culture throughout the CNSS community.

There have been meetings with subject matter experts concerning the DoD Cybersecurity Culture and Compliance Initiative (DC3I) that started in June 2015, and how tactics and procedures from DC3I could prove useful in developing a new CNSS Framework.

The DC3I was created in response to penetrations to non-public information, as well as to the USG reliance on internet and data systems. Some of the key factors behind this initiative were to develop and implement a program to reinforce the traits and attributes of a healthy Cybersecurity culture, such as individual accountability, cybersecurity awareness, and education. One thing CNSS can do to prevent penetrations into NSS is to establish cultural norms to diminish human errors, like negligent security practices out of convenience and improper or delayed network configuration changes.

The CNSS CEWG is determining how to use the DoD's Threat Framework aligned to a cyber kill chain that represents adversarial behavior (tactics, techniques, and procedures) used to analyze the DoD departments' and agencies' Cybersecurity architectures and capabilities to identify gaps and provide recommendations, affirmations, and observations to DoD leaders to improve their Cybersecurity architectures and posture.

The DoD has executed this method of analysis as part of the NIPRNet/SIPRNet Cybersecurity Architecture Review (NSCSAR). Figure 1 below illustrates the components of the NSCSAR efforts and products.

NSCSAR is sponsored by the Department of Defense Chief Information Officer (DoD CIO), the Defense Information Systems Agency (DISA), and the National Security Agency (NSA). The vision of NSCSAR is to leverage the DoD's insight and knowledge to make prioritized cybersecurity capability and informed investment decisions to enable dependable mission execution on the Unclassified and Secret Fabrics. As CNSS is developing and prioritizing its 2017 focus areas, the CEWG will play an important role in developing the 10 priority focus areas for review by the Secret Fabric Governance Board. CNSS will leverage DoD processes, such as DC3I and NSCSAR, and apply them as a baseline within CNSS. They will utilize scorecards to show inadequacies that need to be corrected on the Secret Fabric, as well as provide metrics for issuances.

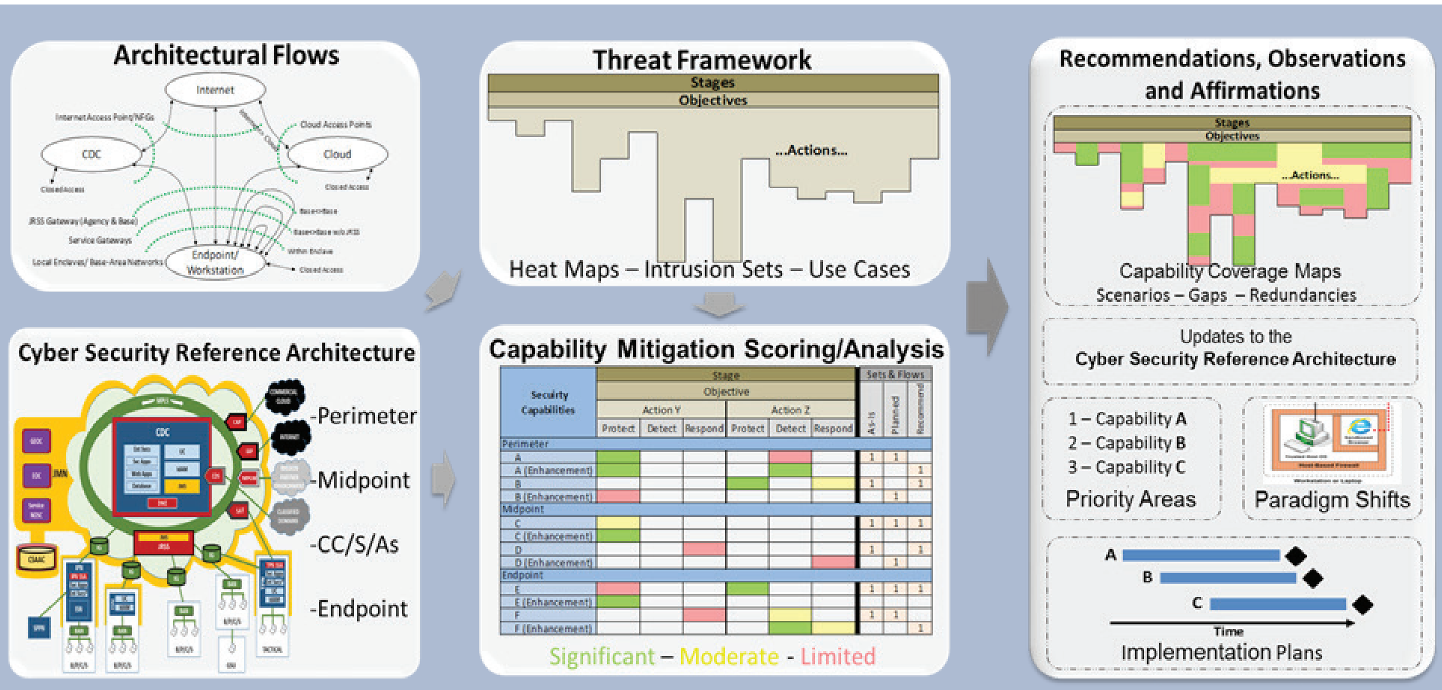
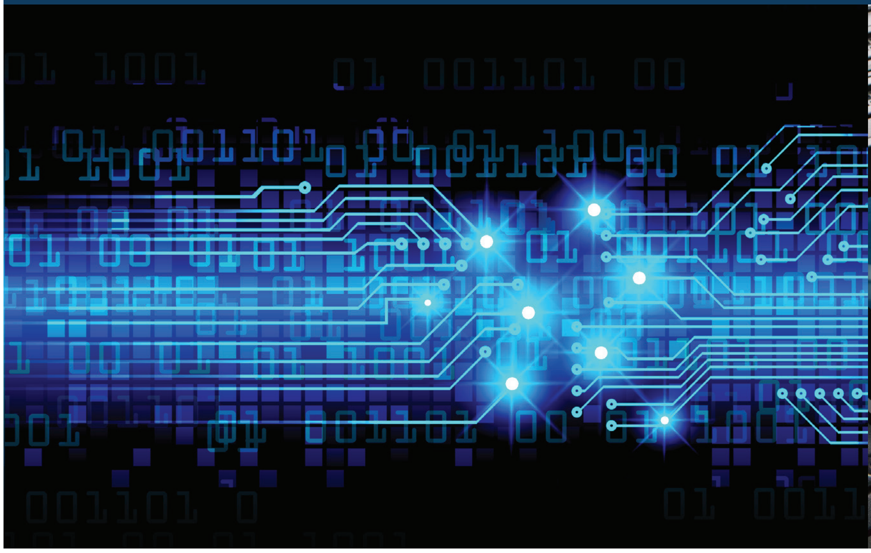


Figure 1 - NSCSAR Concept

The CNSS Subcommittee is investigating how to apply this concept to the broader NSS community to help Federal CIOs make wise investment decisions to protect their systems.

Future Initiatives



CNSS is looking to establish a Secret Fabric Governance Board, pursuant to the provisions of National Security Directive 42, under the authority of the National Manager for NSS. The Board will coordinate closely with the Executive Agent for safeguarding classified information on computer networks and will not infringe upon the authorities related to protection of NSS. The Board will focus on management and oversight of the Federal Secret Fabric as an enterprise. The Board will include representatives from the Executive Branch departments and agencies who are major providers or stakeholders of Secret Fabric networks, and will incorporate participation by information sharing and information assurance, information security, and entities with specific authorities and competences relevant to Secret Fabric governance.

The Board will review, monitor, and provide oversight of NSS network interconnections, Cross Domain Solutions, and of the planned Secret Fabric Cybersecurity Scorecard on behalf of the CNSS Committee, and will make formal recommendations for improvement or for specific remediation to departments and agencies, and to the CNSS Committee.

The Board will also serve as the decision making body for shared risk management and information safeguarding across the Secret Fabric, as well as improving the overall operational management and functionality of information sharing and safeguarding on the Secret Fabric.

DoD and NSA, as the Executive Agent for Safeguarding Classified Information on Computer Networks as defined in E.O. 13587, provides Cybersecurity oversight and independent assessments of NSS. NSD-42 authorizes the Director, National Security Agency (DIRNSA) as the National Manager for NSS to examine USG NSS and evaluate their vulnerability to foreign interception and exploitation. The National Manager is also authorized to operate a central technical center to evaluate and certify the security of NSS. The National Manager is authorized to request from the heads of Executive departments and agencies such information and technical support as may be needed to discharge any of the National Manager’s NSD 42 responsibilities.

Conclusion

As our use of technology to fulfill mission requirements continues to grow and the threats we face continue to evolve, safeguarding NSS remains one of the most crucial elements of our national security posture. The accomplishments highlighted in this report demonstrate the vital role of CNSS and its affiliates in increasing the security of NSS in today's increasingly complex and dynamic environment.

CNSS provides a unique and essential leadership and coordination role among Federal departments and agencies to meet the cyber challenges facing our Nation today and in the future. CNSS promotes interagency coordination and collaboration to develop policies and guidance that will move our Nation toward achieving a common approach for increasing system and network security across the USG for NSS. We must maintain the momentum and continue to work in partnership so that we can leverage existing expertise in meeting current and future cyber security challenges in a unified manner.

CNSS 2016 / 2017 Priorities

Challenge	***Strategy***
Refine and improve CNSS business and issuance development practices.	Use the Safeguarding Working Group (SWG) to: • Assess and update the Privacy, Information, Intelligence, Cross Domain Solutions, Classified Information, and Industrial Control Systems Overlays. • Participate in NIST SP 800-53 rev. 5 update.
Preserve, strengthen, and augment the NSS security baseline.	Use the Governance and Issuance Management Working Group (GIMWG) to: • Prescribe governing and operating procedures for CNSS to establish and ensure uniform management and development of CNSS issuances. • Liaise with CNSS forums to leverage commonalities and promote consistency.
Assess the Cybersecurity compliance and threat readiness of the Federal Secret Fabric.	Use the Compliance and Effectiveness Working Group (CEWG) to: • Utilize DoD's Threat Framework to identify gaps and provide recommendations to improve Cybersecurity architecture. • Leverage DoD knowledge and lessons learned to create and maintain the NSS Secret Fabric Scorecard.
Cybersecurity management and oversight of the Federal Secret Fabric.	Establish a Secret Fabric Governance Board to: • Focus and align the management and oversight of the Federal Secret Fabric as an Enterprise. • Review, monitor, and provide oversight of the Secret Fabric Scorecard. • Assume responsibility for shared risk management and information safeguarding across the Federal Secret Fabric.

DEPARTMENT OF JUSTICE FEDERAL BUREAU OF INVESTIGATION
FIDELITY BRAVERY INTEGRITY
DEPARTMENT OF THE NAVY UNITED STATES OF AMERICA
DEPARTMENT OF TRANSPORTATION UNITED STATES OF AMERICA
JOINT CHIEFS OF STAFF
U.S. DEPARTMENT OF HOMELAND SECURITY
THE DEPARTMENT OF THE TREASURY 1789
DEPARTMENT OF JUSTICE
QUI PRO DOMINA JUSTITIA SEQUITUR
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
OFFICE OF MANAGEMENT AND BUDGET
NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA
DEPARTMENT OF THE AIR FORCE UNITED STATES OF AMERICA
MCMXLVII
DEFENSE INTELLIGENCE AGENCY UNITED STATES OF AMERICA
CENTRAL INTELLIGENCE AGENCY UNITED STATES OF AMERICA
DEPARTMENT OF THE ARMY UNITED STATES OF AMERICA
THIS WE'LL DEFEND
1775
DEPARTMENT OF COMMERCE UNITED STATES OF AMERICA
DEPARTMENT OF STATE UNITED STATES OF AMERICA
GENERAL SERVICES ADMINISTRATION
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE UNITED STATES OF AMERICA
DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA
DEPARTMENT OF THE NAVY UNITED STATES MARINE CORPS
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
DEPARTMENT OF ENERGY UNITED STATES OF AMERICA

CNSS Secretariat
National Security Agency

9800 Savage Road, STE 6165
Fort George G. Meade, MD 20755-6165

410.854.6805 (unclassified phone)

cnss@nsa.gov
http://www.cnss.gov

NATIONAL
SECURITY
ARCHIVE

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu