

UNCLASSIFIED

Statement for the Record

By

Richard H. Ledgett, Jr.

Deputy Director, National Security Agency

Before the

House Armed Services Committee

On the

National Security Agency/Central Security Service

Fiscal Year 2015 Budget

4 April 2014

UNCLASSIFIED

**Introduction**

Chairman Thornberry, Ranking Member Langevin, distinguished Members of the Committee: Thank you for the opportunity to address the National Security Agency/Central Security Service (NSA/CSS) Fiscal Year (FY) 2015 Consolidated Cryptologic Program (CCP), Military Intelligence Program (MIP), and Information Systems Security Program (ISSP) budget. I, and the outstanding men and women of NSA/CSS whom I represent before you today, greatly appreciate the excellent support that the Congress, and this Committee in particular, continually give to NSA/CSS. That support greatly facilitates our mission activities and is instrumental in enabling the many successes that we achieve in our efforts to provide actionable intelligence and information assurance expertise to the diverse customer set that we serve. With your continued support in FY 2015, we will continue to prosecute our mission to protect the Nation and her Allies from those who seek to do us harm.

The FY 2015 NSA/CSS budget reflects hard choices to ensure critical national security requirements are addressed in an era of declining budgets. The Intelligence Community's (IC) highest priority is to provide timely and accurate intelligence support to military, policymakers, law enforcement partners, and allies to keep America and its interests safe and secure. We have recruited and trained an extraordinarily talented workforce, and we must preserve it. We are leveraging our human capital by providing them the most technologically sophisticated and innovative intelligence capabilities. Through focused investment, integration, and efficiency, the IC will sustain responsive and insightful intelligence support as the worldwide threat expands in scope and complexity.

NSA/CSS is well-postured to execute our missions in an operational and technological environment that is complex, and marked by rapid and constant change. As an integral part of America's national intelligence team, NSA/CSS is chartered to lead the U.S. Government (USG) in cryptology by providing Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and enabling Computer Network Operations (CNO) in order to gain a decisive information advantage for national policy makers and war fighting components.

**Strategic Environment**

The strategic environment we face in the years ahead will continue to become more complex and will present a dramatically new set of daunting challenges. The power of information, the speed at which it moves, and its short shelf life in this information age will set the conditions for how NSA/CSS responds to information needs. Transactional, passive, or linear relationships will be replaced by embedded and deeply interactive engagements. Investments in cyber security will expand across the enterprise to meet the demand and speed of action required to thwart our adversaries. The nation will continue to depend upon NSA/CSS to apply cryptography to sustain our access and understanding of data, even as encryption becomes more automatic and prolific. Cyber attacks will continue to offer a means for potential adversaries to overcome overwhelming U.S. advantages in conventional military power and do so in ways that are instantaneous and exceedingly hard to trace. To succeed in this changing environment, SIGINT and IA systems must transform and mature faster than before, and the analytical tools necessary to prosecute these missions must be robust and constantly evolving.

Accordingly, NSA/CSS will pursue the following specific goals:

- Succeed in today's operations by enabling wise policy-making, effective national security action, and U.S. freedom of action in cyberspace via exploitation of foreign electronic signals and systems while protecting privacy and civil liberties;
- Capitalize on technology opportunities to counter increased proliferation and sophistication of encryption, and continue to modernize and streamline Information Technology to improve security, increase capacity and achieve innovative capabilities;
- Prepare for the future by delivering next generation capabilities and solutions that will meet the challenges of tomorrow and drive solutions from invention to operation in support of national security and USG missions;
- Enhance and lead an expert workforce by attracting, developing, and engaging exceptional, diverse personnel prepared to overcome the Nation's hard cryptologic challenges;
- Implement best business practices in order to provide timely data to inform optimal strategic and tactical decisions; and
- Accomplish our missions while maintaining our commitment to compliance, lawfulness, and protection of the public trust.

#### **CCP Initiatives**

The CCP plan provides responsive, reliable, and actionable SIGINT and enables Full Spectrum CNO to provide national policymakers and warfighting commands with the decisive edge needed to keep the Nation safe, while protecting privacy and civil liberties. NSA/CSS global intelligence capabilities, cryptanalysis and analytic tradecraft, operational infrastructure, and information dissemination mechanisms have been developed over time and have resulted in the successful delivery of mission requirements. To strategically posture NSA/CSS to maintain its global capabilities, NSA/CSS will need to: 1) invest in infrastructure, tools, talent, and tradecraft at levels necessary to keep pace with technological changes and changes in target behaviors; and, 2) ensure appropriate balance across the entirety of the Cryptologic platform.

The environment in which NSA operates continues to evolve. Cyber attacks on the US are increasing as access to the Internet expands, IP-based technologies are converging, global telecommunication networks become more diverse, encryption is becoming the standard, and the speed and volume of the internet grows.

To succeed in such an environment, the CCP resource plan will focus on:

- Enabling NSA/CSS to be innovative and creative in developing and sustaining products and services for its customers. The Agency must proactively anticipate the operational landscape and respond with breakthrough technological advances to stay ahead of the target environment and prevent disruptions in intelligence collection.

UNCLASSIFIED

- Maintaining both current and future superiority in the operational environment across mission-priorities. Although there will be changes in tasking consistent with Presidential Policy Directive – 28 (PPD-28), overall the Agency does not expect any significant reduction in customer needs for intelligence.
- Modernization of a uniquely complex enterprise that is engaged in critical and urgent day-to-day operations. In order to bridge current operations into the future operational environment, NSA/CSS must continue to pursue world-class support to current operations even as it strives to gain additional access to key (hard) targets through game-changing cryptanalytic tools and innovative, scalable mission processing and exploitation (P&E) capabilities which enable and support a modernized analysis infrastructure. All of this is required to ensure the ability to provide unfettered analysis of information traversing the volume, variety, and velocity of the 21st century communications infrastructure in order to support the Agency's customers with timely and relevant indications and warnings of adversarial intentions and capabilities.

### **ISSP Initiatives**

NSA/CSS's IA investment plan responds specifically to the 21st century challenge of providing security solutions that keep pace with a fast-moving technology sector, agile adversaries and rapidly-changing customer demands. NSA/CSS IA continuously refines its delivery strategy to provide know-how and technology to suppliers and clients when and where they need it, to measurably improve the security of critical operations and information. The NSA/CSS budget reflects the Department of Defense's increased investment in cyber force/cyber intelligence capabilities.

NSA/CSS has identified five core emphases that will maximize the leverage of its expertise and capabilities:

- Protect information and harden systems in the national security cyber domain: Ensure that national security systems, and others when requested, and the information on or processed by them have the characteristics of confidentiality, authentication, availability, integrity, and non-repudiation, commensurate with known and anticipated risks.
- Shape the operational cyber environment: Know and share understanding of the cyberspace environment and risks. Strategically defend the networks and information critical to national security.
- Maneuver to defend at cyber speed: Know the cyberspace environment and risks; prepare and provide tools and actionable information for others to reconfigure, or when allowed, to reconfigure the cybersecurity posture of national security systems, and other systems when requested, before or during cyber attacks.
- Increase cybersecurity resiliency: Increase the ability to operate; maintain trust in systems and information; sustain mission critical functions in support of cyberspace users; and provide tools and actionable information for others, or when allowed, to rapidly recover or reconstitute full capabilities while experiencing the effects of attacks intending to deny, disrupt, degrade,

UNCLASSIFIED

manipulate, and destroy national security systems, and other systems when such support is requested for them.

- Influence and take maximum advantage of commercial technology: Influence the incorporation of higher security information assurance functions, features, and capabilities into commercial market products supporting USG activities or securing cyberspace of national interest. Incorporate commercial technology and information from the commercial sector into national security systems, and other systems when requested, as well as their operations, while maintaining effective information assurance.

### **MIP Initiatives**

NSA/CSS's MIP investment plan focuses on delivering responsive, reliable, and effective SIGINT products and services to ensure our deployed forces are able to succeed in today's operations and are prepared to respond to future threats and emerging technologies. The NSA/CSS MIP continues previous investments to expand and improve DoD intelligence, reconnaissance, and surveillance (ISR) capabilities as well as increasing the commitment to responding to the cyber challenges of today's world. NSA/CSS will also continue the support of synchronization of tactical SIGINT investments to facilitate an effective joint tactical system that targets the global, converged communications infrastructure. The MIP investments will be focused on strengthening the Department's ability to address current cyber challenges; providing timely and accurate ISR support to our deployed forces; and achieving interoperability, commonality, and modernization of Service and U.S. Special Operations Command SIGINT ISR capabilities.

Specifically, FY 2015 NSA/CSS MIP resource investment will focus on:

- Continuing its investment in a strong cyber workforce and intelligence gathering in cyberspace. These initiatives will focus on providing U.S. Cyber Command Cyber Mission Force (CMF) support, personnel training, and threat operations support and infrastructure.
- Supporting the Defense Intelligence priorities. Investments in the Joint SIGINT mission will facilitate the research and development of tools, systems, software architecture, and solutions that produce actionable SIGINT for deployed forces. Within these areas, there are numerous initiatives that support synchronization and allow for successful joint operations.
- Responding to the need for intelligence support to Combatant Commands (CCMDs). NSA/CSS will continue to invest in efforts which provide SIGINT support to the Commanders. Additionally, operations under this capability will support development of the Operations Plans (OPLANs) and Theater Campaign Plans (TCPs), as directed under Chairman of the Joint Chiefs of Staff (CJCS) Instruction, through extensive planning, modeling, execution, and review of simulation strategies.
- Providing support to the Global Cryptologic Enterprise. NSA/CSS will continue to invest in Real-Time Analytic support. Contained in this effort is RT-RG, or Real-Time Regional Gateway, which

UNCLASSIFIED

will sustain support to the CCMDs, complete migration to the Enterprise Cloud network, and provide analytic capabilities via complex tools and repositories that provide access to large amounts of Near Real-Time (NRT) intelligence.

**Conclusion**

Our budget request reflects the necessary balance between the fiscal realities we face and our commitment to the unparalleled support of the joint warfighter. Moving forward, we will continue to recommend efficient and cost-effective solutions to address intelligence priorities and will remain committed to addressing the challenges posed by our adversaries.

Thank you for your continued support in helping NSA/CSS maintain world-class capabilities and serve as a key contributor to the protection of our nation. I thank you for the opportunity to appear before this esteemed committee and look forward to answering any questions you may have.

UNCLASSIFIED