NSA CYBERSECURITY YEAR IN REVIEW 2024

2024

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
CYBERSECURITY

SECURE OUR FUTURE

CONTENTS

WELCOME

EAST CAMPUS PHOTO COURTESY OF NSA

The National Security Agency (NSA) is the recognized leader in cryptographic capabilities, security engineering and architecture, and advanced cybersecurity guidance and operations. Its mission outcomes produce unique, valued threat intelligence to steer senior actions, investments, and decisions at the highest levels of government, increasing the defensibility of the critical networks and weapons systems belonging to the United States (U.S.).

NSA and its predecessors have protected our country's most sensitive information since World War II. Technological advancements have created a more interconnected world with increasing threats. The future will be dominated by advanced emerging artificial intelligence/machine learning (AI/ML), internet of things, quantum computing, virtualization, Zero Trust (ZT), and cloud technologies; and fifth- and sixth-generation (5G/6G) technological standards for cellular networks.

Drawing on NSA's rich information assurance legacy, NSA's Cybersecurity Directorate (CSD) adapts to meet the demands of the present and future by integrating cryptographic expertise, foreign signals intelligence (SIGINT), vulnerability analysis, defensive operations, and more. NSA established CSD five years ago to scale NSA's cybersecurity mission, achieve greater outcomes, and integrate its efforts to defend against threats like China, Russia, Iran, North Korea, and non-state actors.

NSA secures and manages the infrastructure of millions of devices worldwide. This includes the production and distribution of the keys, codes, and other cryptographic materials that the U.S. Government (USG) uses to secure weapons, satellites, and communications. NSA cybersecurity helps prevent and eradicate threats to U.S. systems and critical infrastructure.

NSA cybersecurity protects and defends the following:

- **Intelligence Community (IC):** This federation of **18** executive branch agencies and organizations focuses on cyber intelligence, counterterrorism, counter proliferation, counterintelligence, and

PHOTO COURTESY OF NSA

threats posed by state and non-state actors that challenge U.S. national security interests worldwide. These organizations, including NSA, work both individually and collectively to ensure the protection of U.S. national security.

- **Department of Defense (DOD):** Headed by the Secretary of Defense, this executive branch department of the USG is the country's largest government agency. The DOD supervises all USG agencies and functions related to national security and the U.S. Armed Forces. NSA is one of **four** national intelligence services under the DOD, alongside the Defense Intelligence Agency, National Geospatial-Intelligence Agency, and National Reconnaissance Office.
- **Federal Civilian Executive Branch:** As the primary interface between the executive branch and the American people, these **102** departments and agencies—which focus on non-military functions—are responsible for delivering fundamental services to the public and supporting the Nation's critical infrastructure. NSA regularly collaborates with these agencies and organizations given their unique roles, ranging from human and financial intelligence to cyber operations.
- **Defense Industrial Base (DIB):** This includes more than **100,000** private-sector technology, manufacturing, and service companies of all sizes that design, develop, and produce critical DOD systems, platforms, and technologies vital to the security of the U.S. and its allies.
- **National Security Systems (NSS):** These telecommunications and information systems contain the Nation's top secrets: classified information, intelligence, and cryptologic activities related to national security; and the command and control of military forces, missions, weapons, and weapons systems. The NSA Director is the National Manager and the CSD Director the Deputy National Manager for NSS. Together, they ensure the USG has a decisive, defensive advantage.

At the end of each fiscal year, NSA releases a Cybersecurity Year in Review to remain transparent in sharing information about efforts that better equipped U.S. defenses against high-priority cyber threats. Visit **NSA.gov/cybersecurity** to access the report digitally. Submit feedback or questions to **cybersecurity@NSA.gov**.

PHOTOS COURTESY OF GETTY IMAGES, EXCEPT: PHOTO 1 (AIRCRAFT) COURTESY OF MASTER SGT. NICHOLAS PRIEST; PHOTO 3 (SUBMARINE) COURTESY OF PETTY OFFICER 1ST CLASS AARON SMITH

PHOTO COURTESY OF NSA

NSA Morrison Center

A LETTER FROM THE NSA CYBERSECURITY DIRECTOR

There's never a dull moment in cybersecurity.

The cyber landscape is defined by change, and threats in this environment have emerged as the number one common denominator among all of our partners. These threats are constantly growing and shifting, as adversaries look to exploit any perceived weaknesses in our collective security.

Our mission is clear: to secure our future, we need to continue detecting, disrupting, and ultimately outmaneuvering cyber threats across the globe.

To do that, we'll need to both scale and integrate our cybersecurity mission. That path requires fully embracing the power of partnerships and leveraging all of our tools and capabilities.

- Partnerships have proven to be a powerful deterrent. Engagement with partners ensures that we can protect critical infrastructure and networks, deliver next-generation encryption capabilities, modernize cross-domain solutions, and disrupt our adversaries' capabilities.
- We will also continue advancing our ability to fully leverage all of NSA's authorities and capabilities to both drive the cybersecurity mission internally, and inform national policy making and incident response efforts across the government.

Cybersecurity is a team sport. It is not the biggest, strongest, or most resourced side that prevails, but the side that can adapt to change the fastest. We are most resilient together.

I'm incredibly proud to serve as the CSD Director. I spend every day with some of the world's finest cybersecurity experts and innovators and I see how their work, together with our partners, is making a real difference in our national security. Throughout this report, you will see just a small glimpse of the daily work that makes CSD a remarkable place. Thank you for reading.

DAVID LUBER
Director, NSA Cybersecurity
Deputy National Manager, National Security Systems

SECURING CRITICAL NETWORKS

PHOTO COURTESY OF GETTY IMAGES

NSA provides foreign SIGINT insights, as well as cybersecurity products and services, to help secure U.S. Military operations and data. NSA produces and distributes the keys, codes, and cryptographic materials that secure **millions** of critical management functions, networks, systems, weapons, satellites, and communications devices worldwide. This includes NSA-certified tactical radios; encrypted solutions used by military critical weapons platforms; and nuclear command, control (NC2) and nuclear command, control, and communications (NC3) systems.

Warfighter Support

NSA supported **1,677** unique customers for critical operations, rapidly deployed over **318** communications security devices to support mission operations during global crises, and delivered **153,749** tamper-indicating products globally that prevent or detect physical exploitation of cryptographic equipment and classified material.

NSA's Commercial Solutions for Classified (CSfC) program is founded on the principle that properly configured, layered solutions can provide acceptable protection of classified data in a variety of different applications. CSfC capability packages provide a robust systems approach that protects NSS for U.S. Military Services, Combatant Commands, and other federal partners. CSfC specifically supported **30** customers this past fiscal year, including the U.S. Army and U.S. Air Force (USAF), North American Aerospace Defense Command, U.S. Northern Command, and Department of Homeland Security.

Office of the National Manager

NSA's Office of the National Manager for NSS was developed to set priorities that enable enhanced security of the Nation's most sensitive systems.

"Protecting our Nation's most sensitive networks includes securing NC3, National Leadership Command Capability, and weapons platforms. CSD partners with the U.S. Strategic Command, USCYBERCOM, and Joint Force Headquarters DOD Information Network to secure these systems and their data, which are vital to the defense of our Nation and allies. We each have unique expertise and authorities that we bring to the fight."

ANDREA RODDY,
NSA Nuclear Command and Control Systems Cybersecurity Chief

INFOGRAPHIC COURTESY OF NSA

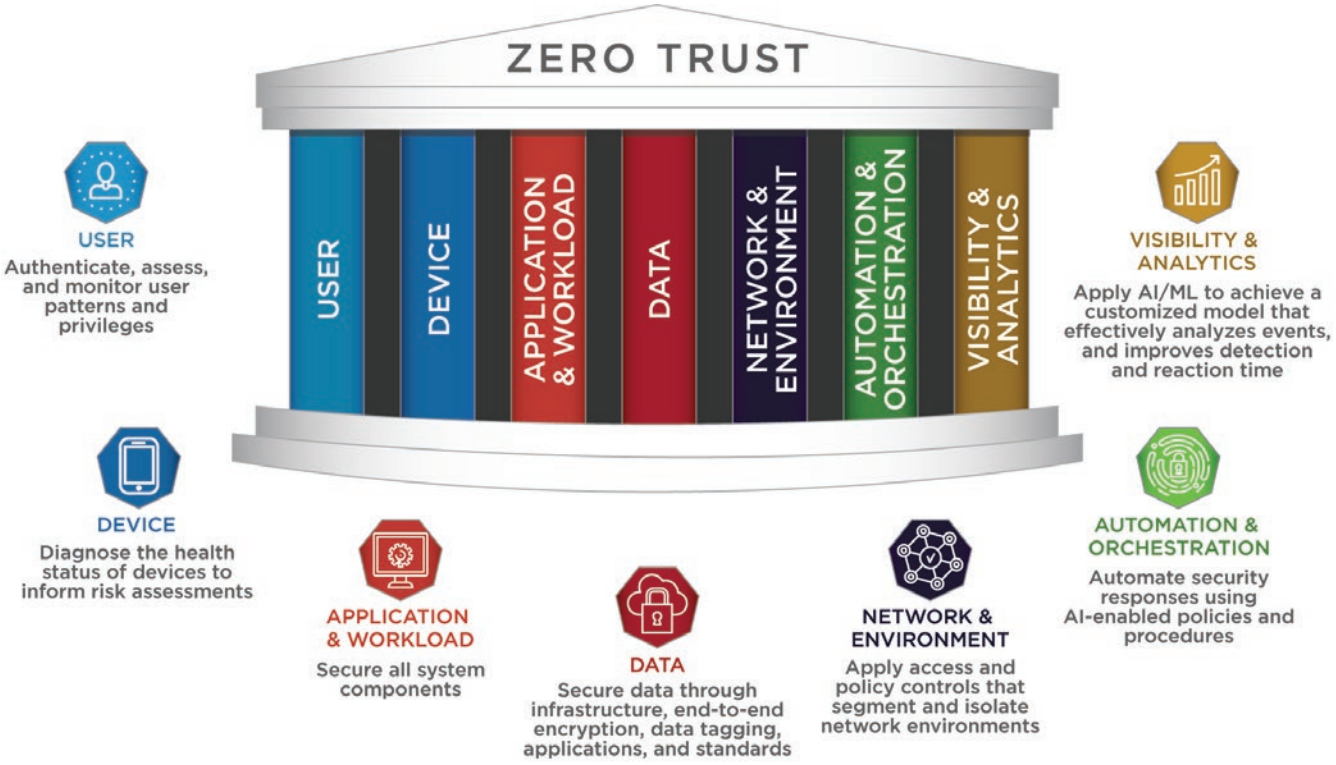
This past year, the office recognized its **one-year** anniversary, highlighting the significant partnerships built within the NSS community. The office participated in over **40** outreach opportunities, focusing on top cyber risks such as ZT, AI, cloud, cross-domain solutions, operational technology, and supply chain security. Additionally, the office released:

- **Twelve Desk Notes recommending vulnerability remediation:** These notified the NSS community of known or reasonably suspected vulnerabilities and threats that, while urgent, did not rise to an emergency threshold.
- **Eight Emergency Directives addressing immediate threats to NSS:** These were released in response to known or reasonably suspected vulnerabilities, incidents, or information security threats to NSS, or intelligence about adversarial capabilities, requiring immediate action and/or mitigation.
- **Three Binding Operational Directives requiring community consideration:** These helped safeguard NSS from known or reasonably suspected information security threats, vulnerabilities, or risks under ongoing monitoring and assessment.
- **Three National Manager Memoranda providing community guidance:** These provided updates and alerts about specific cybersecurity topics.

PHOTO COURTESY OF NSA

Office of the National Manager for NSS Chief Tanya Simms

PHOTO COURTESY OF GETTY IMAGES



INFOGRAPHIC COURTESY OF NSA

Zero Trust

ZT is a security model based on the acknowledgment that threats exist both inside and outside traditional network boundaries. This approach assumes that a breach will occur in systems, and therefore aims to monitor and segment networks in a way that ensures if perimeters and/or systems are breached, adversaries will have limited capabilities to pivot and access critical data. To facilitate the development, deployment, and operations of the ZT framework and security model, DOD guidance organizes ZT capabilities into **seven** pillars that work together to provide a comprehensive and effective security model:

1. User
2. Device
3. Application and Workload
4. Data
5. Network and Environment
6. Automation and Orchestration
7. Visibility and Analytics

NSA published a series of information sheets about how to achieve maturity across the seven pillars, expanding the DOD's framework in a way that made it accessible and practical to organizations of all types as they work to proactively secure their networks more strategically.

NSA's ZT team also conducted expert level on-net/off-net services, and built innovative tools and tradecraft, to drive operations from a reactive to proactive posture. A ZT mindset was adopted in response to the **nine** major perimeter-defense common vulnerabilities discovered across the systems of at least **five** different companies exploited by China this past fiscal year.

"Adversaries will continue to advance in their capabilities. This report demonstrates our commitment to protecting the Nation against the most sophisticated cyber threats."

DAVID LUBER, *NSA Cybersecurity Director*
Deputy National Manager for National Security Systems

NSA CYBERSECURITY REPORTS

COLLABORATIVE. INFORMATIVE. ACTIONABLE.

NSA uses its guidance to highlight current or emerging threats and explain how to protect systems by detecting and mitigating the malicious activity.

NSA collaborates with government and industry to develop and share a comprehensive understanding of nation-state and cybercriminal malicious activity.

NSA and its partners also work together to develop sound defensive measures to secure modern, complicated networks.

Visit **NSA.gov/cybersecurity-guidance** to review NSA's cybersecurity advisories and technical guidance.

Follow @NSACyber on X to receive the latest alerts.

RELEASING ACTIONABLE CYBERSECURITY GUIDANCE

PHOTO COURTESY OF GETTY IMAGES

NSA's cybersecurity publications—Cybersecurity Advisories (CSAs), Cybersecurity Information Sheets (CSIs), and Cybersecurity Technical Reports (CTRs)—provide security guidance and warnings to government agencies, industry, and foreign partners about system vulnerabilities and threat actors. NSA publicly published **43** reports this past fiscal year, most of them jointly with more than **50** other USG agencies and foreign allies. The reports provide curated, focused, and actionable insights to help the national security community protect systems, and are also applicable across critical infrastructure and industry systems.

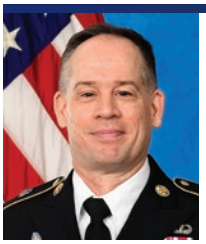
Noteworthy Reports

Volt Typhoon

In 2023, NSA and industry partners identified cyber actor Volt Typhoon (VT) quietly gaining access into critical U.S. infrastructure networks using living off the land (LOTL) tactics, techniques, and procedures to blend in with normal network and system activities and evade detection. To shine light on the VT threat and help network defenders hunt and detect VT malicious activity in their systems, NSA and partners issued a CSA that May titled, "People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection."

In 2024, NSA and its partners published additional insights into VT's pre-positioning for disruptive or destructive cyberattacks against operational technology in the event of a major crisis or conflict with the U.S. A CSA titled, **"People's Republic of China State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure"** noted VT's choice of targets and pattern of behavior. The Cybersecurity and Infrastructure Security Agency (CISA) led the report in partnership with NSA, the Federal Bureau of Investigation (FBI), and other government agencies.

An accompanying CTR titled, **"Identifying and Mitigating Living Off the Land Techniques"** outlined how and why LOTL attacks are effective. This included best practice recommendations as part of a multi-faceted and comprehensive approach to mitigating LOTL cyber threats.



"Calling out suspicious activity helps harden our defenses. We're able to tell net defenders in U.S. and allied governments, critical infrastructure, and private sector organizations where to look, what to prioritize, and how to strengthen their defenses to help keep malicious cyber actors out of their networks."

SERGEANT MAJOR ROBERT SALLINGS,
NSA Cybersecurity Senior Enlisted Leader

"With its SIGINT-backed insight into malicious cyber actors and the ecosystems in which they operate, CSD is uniquely positioned to arm our partners with actionable intelligence that supports national strategic objectives."

DANIEL BARTLETT, *NSA Cybersecurity Adversary Defeat Chief*

Russo-Ukrainian War

NSA, FBI, CISA, and **15** other U.S. agencies and international allies published a CSA titled, **"Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure"** to detail malicious activity used for the purposes of espionage, sabotage, and reputational harm since at least 2020. The authoring agencies assessed that cyber actors affiliated with the Russian General Staff Main Intelligence Directorate 161st Specialist Training Center (Unit 29155) were responsible for the malicious activity. The report included recommended mitigations to improve cybersecurity postures.

Artificial Intelligence

NSA joined the United Kingdom National Cyber Security Centre (NCSC-UK), CISA, and **20** other international allies to release a CSI titled, **"Guidelines for Secure AI System Development."** The report aimed to help developers, providers, and system owners securely design, develop, deploy, and operate AI systems, including those used in NSS, and by the DOD and DIB.

NSA's Artificial Intelligence Security Center (AISC) led the release of its first CSI titled, **"Deploying AI Systems Securely: Best Practices for Deploying Secure and Resilient AI Systems"** to support NSS owners and DIB companies that would be deploying and operating AI systems designed and developed by an external entity. The report is applicable for anyone bringing AI capabilities into a managed environment—especially those in high-threat, high-value settings. Other partners on the release included the following: CISA, FBI, Australian Signals Directorate Australian Cyber Security Centre, Canadian Centre for Cyber Security, New Zealand National Cyber Security Centre, and NCSC-UK.

Cloud

NSA released a compilation of CSIs—collectively the **"Top Ten Cloud Security Mitigation Strategies"**—on different approaches for cloud security mitigation. The CSI for each strategy included an executive summary providing background information and details about threat models. Each CSI concluded with best practices and additional guidance. CISA joined NSA as a partner on **six** of the strategies.

Enduring Security Framework

The Enduring Security Framework (ESF) is a cross-sector working group that operates under the auspices of the Critical Infrastructure Partnership Advisory Council. The group addresses threats and risks to the security and stability of NSS and critical infrastructure. USG experts and representatives from the IT, communications, and DIB sectors participate. NSA is the ESF Executive Secretariat. In fiscal 2024, the ESF published the following:

- **"Securing the Software Supply Chain: Recommended Practices for Managing Open-Source Software and Software Bill of Materials" / "Securing the Software Supply Chain: Recommended Practices for Software Bill of Materials Consumption"**
- **"Recommendations for Increasing U.S. Participation and Leadership in Standards Development"**
- **"Identity and Access Management: Developer and Vendor Challenges"**

PHOTO COURTESY OF NSA

Russian activity in Ukraine, AI/ML, and cloud technologies were among the topics discussed in the second episode of NSA's official public-facing "No Such Podcast" titled, "Cybersecurity is National Security" featuring Luber and former CSD Deputy Director for Combat Support Lieutenant General Melvin "Jerry" Carter

LEVERAGING THE POWER OF PARTNERSHIPS

PHOTO COURTESY OF NSA

Left to right: Five Eyes partners Lisa Fong (New Zealand National Cyber Security Centre), Luber, Stephanie Crowe (Australian Signals Directorate), Felicity Oswald (United Kingdom National Cyber Security Centre), and Rajiv Gupta (Canadian Centre for Cyber Security)

NSA's **industry, academic,** and **government partners** are force multipliers in cyber space—when we work together, we are all stronger.

Industry

Cybersecurity Collaboration Center

A unique space that embraces constant collaboration in real time.

The Cybersecurity Collaboration Center (CCC) leads NSA's efforts to partner with large DIB companies and their service providers. Equipped with a strong perspective on nation-state actors' plans and intentions, the CCC shared threat intelligence, compromise indicators, and vulnerability assessments throughout the year—a form of persistent deterrence.

The CCC led bi-directional and multi-lateral sharing with partners that have significant global reach and the ability to help NSA scale cyber defense measures by sharing insights regarding malicious activity they observe in their own networks.

In just four years, the CCC's industry partnerships have grown from just one to more than **1,300**—including prime DIB companies. NSA has scaled prevention, detection, and mitigation techniques to **billions** of endpoints worldwide. This past year, NSA enhanced its understanding of threats and established over **800** collaboration channels featuring around **35,000** analytical exchanges. Countering the U.S.'s strategic competitor, NSA made significant strides to outmaneuver China's cyber targeting of U.S. critical infrastructure, working with industry and using its intelligence capabilities to actively monitor actors, notify organizations of compromises, share details of

"Partnerships are at the core of what we do. Working so closely with our partners—sharing critical, timely information across industry, academic, and government lines—has been a game-changer. By expanding our partnership network from just one company four years ago to over 1,300 partners today, we are working to ensure NSA's insights and expertise reach the DIB at an unprecedented speed and scale."

KRISTINA WALTER, *NSA Cybersecurity Collaboration Center Chief*

BY THE **NUMBERS**

≈154,000
tamper-indicating products

+1,300
DIB industry partners

≈50
career fairs and professional events

≈35,000
analytical exchanges

+800
collaboration channels

+40
actionable joint publications

≈1,700
unique customers

≈500
NCAE-C-designated higher-ed institutions

≈30
SDA low-Earth orbit satellite launches supported

malicious tradecraft, and expose zero-day exploits to software vendors for patching.

A few examples of partnership in action:

- The CCC helped illuminate China exploiting vulnerable devices to target the DIB by issuing unclassified, actionable detection and mitigation guidance to all DIB partners based on the collaboration and industry feedback.
- Informed by multiple industry tips, NSA also discovered computer network exploitation actors attempting to scan and enumerate DIB infrastructure associated with a known vulnerability. The CCC quickly provided notifications to the DIB partners in advance of any detectable compromise. Further collaboration revealed additional infrastructure and tactics, techniques, and procedures used by China-sponsored actors.
- The CCC helped an industry partner discover a VT actor (cited under the *Releasing Actionable Cybersecurity Guidance* section of this report) targeting a U.S.-based cybersecurity company supplying software to the U.S. Military.
- By leveraging threat intelligence shared by a cybersecurity industry partner, the CCC was able to quickly tip targeted DIB companies to a malicious social engineering campaign. Those impacted were provided with timely and unique information, which enabled them to respond and/or identify activity targeting their company and its employees.

Cybersecurity-as-a-Service

This year, NSA made significant strides in shoring up the DOD supply chain as the NSA CCC hit a milestone: **1,000** unique companies enrolled in its DIB Cybersecurity-as-a-Service (CSaaS) program.

This program is how NSA provides direct cybersecurity assistance to small businesses that support critical DOD programs.

This protects sensitive but unclassified DOD information that sits on privately owned and managed networks, which are likely to be targeted by sophisticated nation-state adversaries. By providing NSA analytic and technical expertise to these small companies, NSA is giving them a leg up in what would otherwise be a fundamentally unfair fight.

NSA offered this initial set of refined core services:

1. **Protective Domain Name System** blocks users from connecting to known malicious domains by running every query through NSA-enriched threat feeds prior to resolving those queries.
2. **Attack Surface Management** helps DIB companies find and mitigate vulnerabilities in their internet-facing assets. While many malicious cyber actors—ranging from ransomware to state-sponsored actors—leverage publicly-known, internet-facing vulnerabilities to gain initial access to their victims, this service helps DIB companies find and fix issues prior to comprise.
3. **Threat Intelligence Collaboration** is how NSA shares non-public, DIB-specific threat information with those companies and welcomes specific questions from them directed at NSA analysts.

A fourth service was added this year:

4. **Autonomous Penetration Testing** leverages AI to automate and replace manual processes associated with penetration testing. Machine-driven penetration tests integrate cutting-edge research on the newest vulnerabilities, and enable the identification of issues often well before attackers create exploits. DIB customers can run a penetration test of their internal assets, identify issues, implement mitigations, and confirm they effectively closed the discovered holes. A small NSA pilot found that participating DIB companies identified more than **25,000** internal network vulnerabilities and swiftly resolved **thousands** of high-criticality vulnerabilities. This service will be scaled to any interested and qualifying DIB company.

The CCC launched new campaigns to provide analytic support to semiconductor manufacturing companies. The CCC organized outreach around strategic campaigns aligned to DOD priorities that focused on priority weapon supply chains and companies in regions of interest, such as those involving the ongoing Russo-Ukrainian conflict and others critical to Pacific defense.

The CCC also extended cybersecurity support to more than **50** contracted carriers providing mission-critical components and services to the U.S. Transportation Command, including ocean and

intermodal cargo transport, heavyweight delivery, and military airlift. As a result of these partnerships, NSA identified multiple contractors with known software vulnerabilities, in addition to emerging malicious cyber actors attempting to exploit those vulnerabilities. Successful exploitation could have resulted in remote code execution on DIB companies' networks. NSA immediately alerted the companies, which responded within hours, having successfully patched their assets and confirmed that no compromise had occurred.

The CCC extended this same support to more than **20** U.S. European Command suppliers providing mission-critical components and services such as tactical and satellite communications equipment, disaster relief, power supplies, and electronic warfare mission systems. For these companies alone, the CCC's program blocked over **3.4 million** threats, **3.2 million** of which were directly from NSA-provided indicators of compromise.

Center for Cybersecurity Standards

The Center for Cybersecurity Standards (CCSS) is focused on authoring, informing, and driving adoption of standards to secure NSS and the DIB. Increased U.S. participation in standards development organizations (SDOs) is critical to protecting the security of the American people, expanding economic opportunity, and defending democratic values.

NSA engaged in more than **15** SDOs and submitted over **70** standards submissions within these organizations in the past year. For example, the CCSS contributed to standardizing critical and emerging technologies like AI while participating in the International Organization for Standardization/ International Electrotechnical Commission Subcommittee 42.

NSA also hosted the second National Security Standards Summit at the CCC, gathering together more than **138** standards experts across the USG, foreign partners, industry, and academia. These subject matter experts (SMEs) engaged in in-depth discussion on standards for technologies critical to national security and development challenges.

Leveraging deep technical cybersecurity expertise, the CCSS works to establish safe, interoperable, and secure global standards for critical telecommunications technologies. The CCSS coordinated with liaisons from the International Telecommunication Union and 3rd Generation Partnership Project to thwart Russian attempts to move 5G authentication work outside of organizations and away from experts most equipped to address vulnerabilities. This ensured that standardization remained in the hands of the appropriate technical experts as opposed to state actors.

"Partnerships are our superpower. Working with partners, we're able to see around corners, identify blind spots, and piece together the full picture of threats we see. We then collaborate on solutions that not only protect the networks and systems that NSA cares about, but also the ones our partners patch to protect all their customers. It's how we detect and defend at scale."

JEREMY SANSBURY, *NSA Cybersecurity Deputy Director*

National Information Assurance Partnership

The National Information Assurance Partnership (NIAP) oversees evaluation of commercial, off-the-shelf (COTS) IT products for use in NSS.

The NIAP continued to strengthen global partnerships by representing the U.S. in the Common Criteria Recognition Arrangement (CCRA), a **31**-member international body dedicated to the certification of COTS products. The NIAP also hosted the annual CCRA meeting in Washington, D.C., bringing together **18** nations to update mutual recognition agreements and address global product evaluation and certification concerns. Similarly, the NIAP led the successful periodic assessment of the Indian Common Criteria Certification Scheme to ensure that the CCRA maintains trust and confidence in the shared evaluations between the nations.

Through the NIAP, the CCC certified **72** commercial components for protecting NSS, and the NIAP published **seven** Protection Profiles to raise security in those products.

Leveraging strong, global relationships, the NIAP coordinated with international partners to expand product certification to include additional critical technologies, beginning the first-ever Common

Luber at the CCC

Examples of joint cybersecurity publications that NSA contributed to

PHOTOS COURTESY OF NSA

Criteria cloud product evaluation and developing a Software-Bill-of-Materials pilot with vulnerability tracking designed to improve supply chain security.

Academia

NSA continues to inspire future cyber warriors through initiatives like its Codebreaker Challenge, GenCyber program, Cyber Exercise, and Experiential Tours.

The Agency had **214** Education Partnership Agreements and **79** Cooperative Research and Development Agreements with higher educational, kindergarten through 12th grade-level, and not-for-profit/non-profit institutions that were active and continuing by the end of the fiscal year, having increased the former by **48** and latter by **22** from the previous fiscal year.

NSA deployed **187** academic liaisons who engaged with nearly **287** colleges and universities across the country, having increased the numbers by approximately **40** liaisons and **50** schools from the previous fiscal year.

Additionally, NSA remains invested in promoting cybersecurity careers throughout all levels of education through its National Cryptologic University (NCU), which runs the National Centers of Academic Excellence in Cybersecurity (NCAE-C) program. This program:

- **Establishes standards** for cybersecurity curriculum and academic excellence.
- **Includes competency** development tactics among faculty and students.
- **Values community outreach** and leadership development.
- **Integrates cybersecurity practices** across academic disciplines.
- **Actively engages** in solutions facing cybersecurity education.

Nearly **500** schools have received the NCAE-C designation in the fields of cyber, cyber defense, and cyber research. Additional details can be found in the *Building and Sustaining an Expert Workforce* section of this report.

Government

NSA scaled its efforts to counter China and Russia through cyber diplomacy. Meanwhile, the demand for cyber intelligence sharing and cybersecurity assistance from partner nations across all Combatant Commands has increased. NSA's cybersecurity teams repeatedly rose to the occasion, partnering with federal cyber centers to collaborate daily and maintain uninterrupted 24/7 cybersecurity operations. By fostering close partnerships, NSA successfully shares critical cyber threat indicators, empowering allies to proactively counter cyber adversaries.

Improve Network Defense

NSA's no-cost DIB services will help increase the security of your networks.

GET STARTED TODAY

NSA.gov/CCC

NATIONAL SECURITY AGENCY · UNITED STATES OF AMERICA

CYBERSECURITY COLLABORATION CENTER

TRANSITIONING TO QUANTUM-RESISTANT CRYPTOGRAPHY

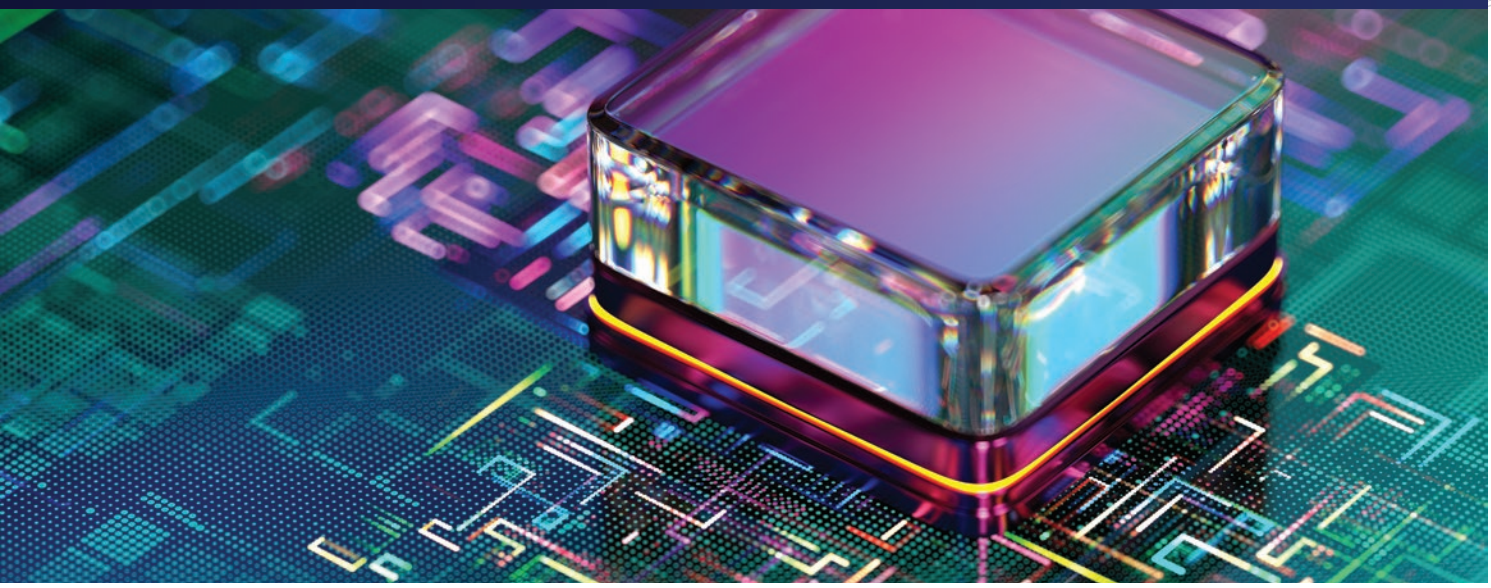


PHOTO COURTESY OF GETTY IMAGES

NSA continues to develop and adopt new technologies across its various mission platforms. Working closely with the National Institute of Standards and Technology (NIST) and other partners to ensure the protection of the Intelligence Community (IC) from quantum threats, NSA delivered rapid cryptographic support and increased the security of network connectivity for intelligence sharing.

NSA updated security evaluation requirements that raised the bar for vendors regarding their development of cryptography to defend against quantum computing and comparable threats. It provided updates to security requirements and architectures to combat evolving adversarial capabilities, tools, techniques, and processes.

"A lot of folks think that cybersecurity is just the IT systems that everyone has on their desktop, servers, or cloud. In reality, cybersecurity also supports and surrounds our weapons and space systems for both current and future use. Our cryptography is literally out of this world."

JEFFREY DICKERSON, *NSA Cybersecurity Technical Director*

Subsequently, NSA undertook a series of product developments that aligned with updated guidance to deliver a set of next-generation devices for the post-quantum computing era, releasing an updated cryptographic modernization roadmap with product implementation timelines.

NSA also focused on ensuring its quantum-resistant cryptography would successfully protect NSS by completing a large-scale, multi-year modernization effort to prepare for the era of quantum computing. This involved updating outdated NC2, NC3, and key management infrastructure systems. NSA continued to enhance the overall cybersecurity posture of NSA's critical infrastructure systems through various equipment upgrades and highly focused efforts. NSA modernized its ability to distribute cryptographic keys through secure, high-assurance communications software practices for all weapon systems and military operations, and collaborated with the DOD and DIB to update encryption across the U.S. Combatant Commands to reduce adversarial access to warfighter communications and sensitive data.

Space

The use of proliferated low-Earth orbit architectures to support warfighters has demonstrated the need to scale space system security. NSA continued work to ensure that high-assurance cryptography protects all parts of the IC and DOD space ecosystem,

and made great strides toward achieving next-generation encryption solutions.

Link-16 is a military communication system used to transmit and exchange real-time information between military aircraft, ships, and ground forces. NSA supported the Space Development Agency (SDA) in deploying the first-ever Link-16 command and control capabilities for weapons systems in space.

NSA also helped develop a cryptographic solution for proliferated space mesh constellations networks. These are architectures of multiple, smaller, and often more cost-effective satellites performing several functions such as dynamic network routing, switching, collecting, processing, and data transferring. These functions involve distributing data and balancing loads with other space assets rather than relying on a few large, expensive satellites. This improves resilience, coverage, and functionality of space systems. For defense applications, satellite mesh constellations enhance situational awareness and strategic advantages through distributed capabilities that are harder to disrupt. Overall, NSA supported the SDA's **27** low-Earth orbit satellite launches this past fiscal year.

PHOTO COURTESY OF GETTY IMAGES

PHOTO COURTESY OF GETTY IMAGES

NSA also continued its support of the U.S. and its allies for critical operations, such as providing global positioning system cryptographic keys for the U.S. Space Command. NSA cybersecurity vulnerability analysts partnered with the USAF to analyze a commercial aircrew support product. The collaborative effort's findings led to the development of improved system security and data protection guidance that immediately supported active platforms globally and helped shape future uses.

Whether it is satellite command, control, and communications; mission operations; or hand-held, mounted, connecting, and space segments, efforts like these enhance warfighter support and introduce new communications capabilities. This empowers the warfighting capability to sense, diagnose, and act alongside partners at all levels, through all phases of war, and across all domains to deliver information advantages at the speed of relevance.

"Collaboration is essential in moving toward quantum-resistant compliance. The government and industry must continue the journey together to modernize cryptography to defend our Nation against the looming quantum threat."

CEDRIC TERRY,
NSA Cybersecurity Encryption Production and Solutions Chief

EXPLORING ARTIFICIAL INTELLIGENCE

PHOTO COURTESY OF GETTY IMAGES

A growing and complex field, AI security is about protecting AI systems from learning, doing, and revealing data that could cause harm to national security. NSA is bringing its deep technical expertise and insights, unique partnerships, and authorities to whole-of-government and private efforts to ensure the U.S. has an enduring advantage in this area.

AI is allowing adversaries to increase the speed, scale, and sophistication of offensive cyber capabilities. They are able to conduct spearphishing to gain access into our networks, create deepfakes to erode confidence in our democracies, and assist nation-state cyber actors as co-piloting hackers during computer network operations to strengthen their offensive strategies.

AI technologies are also being developed and proliferating faster than companies and governments can shape norms and standards. Standards directly underpin national security and the economy by integrating security into early product development, reducing the risk of manufacturers and their customers becoming victims of exploitation due to insecure or weak technologies. This allows for interoperability between technologies so that the U.S. is not reliant on single-market vendors. As AI is increasingly implemented in NSS and DIB networks, the security of those AI systems becomes especially important.

Artificial Intelligence Security Center

Building on the success of the CCC's partnership model, the NSA launched the Artificial Intelligence Security Center (AISC) as a new branch of the CCC in September 2023. The AISC is focused on promoting the secure development, integration, and adoption of AI capabilities within NSS and the DIB. NSA's principles, values, and culture of compliance serve as the foundation for AISC activities.

"NSA's AISC created a space where we can build critical partnerships and share threats, best practices, and research across the AI industry to stay ahead of how adversaries use and target AI. Just as we saw when we started building the CCC, combining NSA's expertise with a forward-leaning partnership model allows us to capture, learn, and share at the cutting edge to protect NSS and the DIB."

TAHIRA MAMMEN, *NSA Artificial Intelligence Security Center Chief*

PHOTO COURTESY OF NSA

CSD's AISC Chief Tahira Mammen during the third episode recording of NSA's "No Such Podcast" titled, "AI and the Future of National Security"

PHOTO COURTESY OF NSA

Research Director Gilbert Herrera with expert Dr. Kathryn Baker in NSA's fifth podcast episode, "The Cutting Edge of Classified: Research at NSA"

The AISC is focused on three main objectives:

1. **Detecting and countering foreign threats** that would impact AI systems we would want to use in our NSS.
2. **Developing deep partnerships** with those across the national security community (i.e. AI vendors and users) that would want to use and implement AI for either warfighting or IC capabilities.
3. **Defining and promoting best practices,** guidelines, principles, evaluation methodologies, and risk frameworks for AI security.

Serving as NSA's focal point for leveraging foreign intelligence insight, the AISC works closely with U.S. industry, national laboratory, academic, IC and DOD, and select foreign partners to better understand threats to intellectual property.

The AISC will be integral to preventing malicious foreign actors from our country's innovative AI capabilities.

Cybersecurity Research

NSA partners with a rich set of government, academic, national laboratory, non-profit, and industry researchers, practitioners, and management leaders to conduct advanced research in cybersecurity and apply successful research results towards advancing NSA's cybersecurity mission. Annual forums foster sustainable research communities by creating opportunities for dialogue centered around the development of scientific foundations for the engineering and analysis of complex computing systems and data.

NSA's Laboratory for Advanced Cybersecurity Research creates groundbreaking science and delivers transformative capabilities at the intersection of cutting-edge research in cybersecurity and AI. Work in this space enables NSA to effectively anticipate and deliver based on current and future operational needs, and advance strong, flexible operating system security mechanisms. For example, multiple computing providers publicly announced the adoption of security-enhanced Linux (SELinux)—NSA's first released open-source software—features to harden their cloud infrastructures. This year marked the 20th anniversary of SELinux as a default-enabled security feature, including for over **three billion** active Android devices. NSA also successfully transitioned Linux Kernel Integrity Measurer technology to commercial products and mission partners to enable signature-free detection of kernel implants for Linux-based systems.

PHOTO COURTESY OF NSA

BUILDING AND SUSTAINING AN EXPERT WORKFORCE

PHOTO COURTESY OF GETTY IMAGES

Threats to the Nation never cease, and neither does the work to counter them. The collective, multi-disciplinary expertise of NSA's robust cyber workforce, combined with its culture of ingenuity, make it invaluable to the Nation. NSA observed an increased demand for skills in science, technology, engineering, and mathematics (STEM) disciplines—particularly pertaining to cybersecurity—and prioritized outreach and skills-based hiring to recruit and retain its talented personnel. NSA led academic outreach initiatives targeting STEM/cyber programs at regionally accredited colleges and universities, and participated in speaking engagement events ranging from national cyber conferences and summits to kindergarten through 12th grade-level cyber competitions.

> "While I was on the offensive side of cyber, I thought that's what it was all about, but the game is really played on the defensive side. What we do in CSD is going to make or break the Nation for the next 10 to 15 years… and it all starts with investing in ways to preserve the talented workforce we have and recruit the next-generation of cyber experts to tackle the challenges of tomorrow."

BRIGADIER GENERAL WILLIAM "WILL" WILBURN, JR.,
NSA Cybersecurity Deputy Director for Combat Support

Recruitment

NSA designed robust initiatives to attract an array of candidates not just with cybersecurity backgrounds, but a broad range of specialties. The Agency hosted "NSA in Focus" virtual webinars, enabling candidates to hear from employees about career experiences. NSA discussed the importance of developing a resilient, future-ready cyber workforce on the first season of NSA's official public-facing **"No Such Podcast"** in the second episode titled, **"Cybersecurity is National Security."**

NSA participated in nearly **50** in-person and virtual college/university career fairs and professional events across the country to attract cybersecurity STEM majors to apply for both internship and employment opportunities. NSA also recruited and processed talented applicants who fell victim to technical sector layoffs. Candidates were recruited at several events throughout the year.

Programs

- **NCAE-C Program:** Managed by the NCU with community colleges and universities, this NSA program establishes standards

for cybersecurity curriculum and academic excellence. NCAE-C schools benefit from competency development among students and faculty, community outreach, leadership in professional development, integrated cybersecurity practices within institutions and across academic disciplines, and engagement in solutions to challenges facing cybersecurity education. Learning through cyber clinics, competitions, and technical student organizations to complement and establish credit towards programs of study through the NCAE-C is also underway.

"The strength of NSA cybersecurity lies in our ability to recruit, hire, and retain a talented workforce with a variety of work experiences. Whether you arrive directly out of school or after years of industry experience, you'll be part of a team of professionals providing cutting-edge security on behalf of the Nation."

CARMINE APICELLA, *NSA Cybersecurity Chief of Staff*

- **DOD Cyber Scholarship Program:** Funded by the DOD Chief Information Officer and administered by NSA, this program recruits high school students to attend educational institutions with the NCAE-C designation on scholarships and eventually work for the federal government. It demonstrates DOD and congressional commitments to support higher education so that the DOD workforce is prepared to handle threats against critical information systems and networks. The retention option, under which DOD civilian employees and military members may apply for full-time graduate or part-time undergraduate programs, was reinstated.
- **GenCyber Program:** This annual competitive program is offered by NSA and the National Science Foundation to designated educational and non-profit organizations that partner with an academic institution. The program provides year-round cybersecurity opportunities to students and teachers at the secondary level. Proposers can submit for **three** types of programs: student, teacher, and combination. This past year, **86** programs (**55** students/**29** teachers/**two** combinations) were funded across **43** states, plus Washington, D.C. and Puerto Rico, serving approximately **2,000** students and teachers.
- **U.S. Marine Corps Forces Cyberspace Command (MARFORCYBER) Cyber Apprenticeship Program:** MARFORCYBER is the U.S. Marine Corps component to USCYBERCOM. This program gives students an opportunity to work in offensive, defensive, and supporting operations in cyber space. For example, NSA secured a CSD position for a recent graduate.
- **NSA Experiential Tour (NET) Program:** This provides early and continued exposure to SIGINT and cybersecurity missions, aiming to garner interest from a new generation of military leaders. Cadets, midshipmen, and select civilian students are recruited from across the **four** U.S. Service academies, **six** senior military colleges, and nationwide Reserve Officer Training Corps programs. Each participate in a **four- to six-week** tour under the mentorship of a NSA SME with one of the NET's strategic partners, including the USCYBERCOM, MARFORCYBER, FBI, and many others. Having hosted over **220** participants this past year, the NET program continues to grow annually, its success attributed to the expansion of strategic partnerships within the IC and DOD. These are foundational to the NET program goals of developing the expertise required to support a future-integrated IC mission.

PHOTO COURTESY OF NSA

Walter engaging with NSA program participants

PHOTO COURTESY OF GETTY IMAGES

Exercises

- **National Collegiate Cyber Defense Competition:** Sponsored by NSA cybersecurity and operations, this highly competitive cyber task force brings together the top scholastic cyber clubs in the country to compete in real-world scenarios and provides an opportunity to engage with various schools and increase NSA's academic engagement footprint.
- **NSA Cyber Exercise (NCX):** Held in coordination with USCYBERCOM, the NCX trains future military and civilian cyber warriors and leaders by developing and testing their cybersecurity, teamwork, planning, communication, and decision-making skills. This annual exercise is the competitive cyber event of the year for U.S. Service academies, senior military colleges, and NSA professional development program participants. This past year, the competition resumed in person for the first time since the COVID-19 pandemic. Teams were challenged with solving a physical hardware issue, with a surprise continuity of operations element adding to scenario's realism. The U.S. Military Academy won the exercise and was awarded the 2024 NCX trophy. NSA hiring managers provided participants with an overview of NSA's hiring process, including specifics to military members considering a transition to civilian employment.
- **NSA Codebreaker Challenge (CBC):** Launched in 2013 to just **five** schools, NSA CBC celebrated its **10th** year, reaching **thousands** of participants. The annual CBC provides a forum for students from U.S.-based academic institutions to explore real-world scenarios that emulate the IC's classified work environment. The challenge prepares participants to tackle national security concerns and advance their skills in reverse engineering, vulnerability analysis, cryptanalysis, research, and exploitation. Participants in the most recent challenge sharpened their skills by interpreting and discovering the origin of an unknown signal identified by the U.S. Coast Guard. They were presented with a series of **nine** increasingly complex tasks to locate and analyze where the signal originated, discover an active collection operation tasked by a rogue server, and subvert the server to stop the collection device.

These programs and exercises reflect CSD's ongoing commitment to hire an expert workforce.

Retention

NSA continues to advance its next generation of expert mathematicians to ensure cryptography is secure by providing its workforce with professional development opportunities in the form of advanced training and crypto-mathematical guidance and analysis. NSA's Cybersecurity Cryptographic Evaluation organization teaches **nine** NCU courses to employees and other members of the IC, and won NSA's 2023 Crypto-Mathematics Institute Teaching Award for developing and teaching the "Vulnerabilities in Cryptographic Implementations" NCU class. NSA specialists in cryptanalysis, signals analysis, research, target pursuit, and computer network operations benefit from these courses. NSA also organizes various workshops covering post-quantum, symmetric, and advanced cryptography, as well as side-channel analysis.

ACRONYM GLOSSARY

5G/6G Fifth- and Sixth-Generation

AI/ML Artificial Intelligence/Machine Learning

AISC NSA Artificial Intelligence Security Center

CBC NSA Codebreaker Challenge

CCC NSA Cybersecurity Collaboration Center

CCRA Common Criteria Recognition Arrangement

CCSS Center for Cybersecurity Standards

CISA Cybersecurity and Infrastructure Security Agency

COTS Commercial Off-the-Shelf

CSA Cybersecurity Advisory

CSAAS Cybersecurity-as-a-Service

CSD NSA Cybersecurity Directorate

CSfC Commercial Solutions for Classified

CSI Cybersecurity Information Sheet

CTR Cyber Technical Report

DIB Defense Industrial Base

DOD Department of Defense

ESF Enduring Security Framework

FBI Federal Bureau of Investigation

IC Intelligence Community

IT Information Technology

MARFORCYBER U.S. Marine Corps Forces Cyberspace Command

NC2 Nuclear Command, Control

NC3 Nuclear Command, Control, and Communications

NCAE-C National Centers of Academic Excellence in Cybersecurity

NCSC-UK United Kingdom National Cyber Security Centre

NCU National Cryptologic University

NCX NSA Cyber Exercise

NET NSA Experiential Tour

NIAP National Information Assurance Partnership

NIST National Institute of Standards and Technology

NSA National Security Agency

NSS National Security Systems

SDA Space Development Agency

SDO Standards Development Organization

SELinux Security-Enhanced Linux

SIGINT Signals Intelligence

SME Subject Matter Expert

STEM Science, Technology, Engineering, and Mathematics

U.S. United States

USAF U.S. Air Force

USCG U.S. Coast Guard

USCYBERCOM U.S. Cyber Command

USG U.S. Government

VT Volt Typhoon

ZT Zero Trust

www.NSA.gov/cybersecurity