

2021

NSA Cybersecurity
Year in Review



Welcome

The National Security Agency (NSA) formed a Cybersecurity Directorate in 2019 with the charge to prevent and eradicate threats to the United States' National Security Systems and critical infrastructure, with an initial focus on the Defense Industrial Base and its service providers.

Drawing on NSA's rich information assurance legacy, the Cybersecurity Directorate refocused to meet the demands of the present and the future. It integrated key parts of NSA's cybersecurity mission such as threat intelligence, vulnerability analysis, cryptographic expertise and defensive operations into a more public-facing organization determined to raise the cybersecurity bar across government and industry while also imposing cost on U.S. adversaries.

While much of the critical work that NSA does to secure the nation cannot be publicly disclosed, this year in review shares a wealth of information on cybersecurity efforts that have better equipped the U.S. to defend against the highest priority cyber threats from November 1, 2020 through October 31, 2021.

Visit [NSA.gov/cybersecurity](https://www.nsa.gov/cybersecurity) to access the report digitally. Provide NSA Cybersecurity with feedback or ask questions by emailing cybersecurity@nsa.gov

NSA Cybersecurity Protects and Defends

National Security Systems (NSS)

Networks that contain classified information or are otherwise critical to United States military and intelligence activities. It is vital that these networks remain secure to ensure mission readiness of U.S. warfighting capabilities as well as protect the nation's most sensitive information.

The Department of Defense (DoD)

U.S. military services and combatant commands as well as U.S. government agencies and departments related to national security.

The Defense Industrial Base (DIB)

Companies that design, develop and produce the Department of Defense's critical systems, platforms and technologies required to defend the nation. If these networks are at risk, so is the U.S.

Contents

3 Letter from the NSA Cybersecurity Director

4 Responding to National Threats and Priorities

7 Partnering to Secure Today and Tomorrow

10 Sharing Timely, Actionable Guidance

12 Protecting the Warfighter and Supporting the Combatant Commands

16 Creating Cryptography to Protect Data, Communications

19 Defending National Security Systems

22 Building a Diverse Workforce That Can Tackle Any Challenge



Letter from the NSA Cybersecurity Director

When our insights are brought into a feedback loop with industry and government partners, amazing outcomes are achieved. We create impact far beyond what any of us can do alone.

Cyber threats to our nation rose to national consciousness this past year. We felt the real-world consequences that malicious cyber actors can inflict from cyberspace. We saw how malicious cyber actors will infiltrate global supply chains as well as exploit popular applications for ransomware. We even saw how ransomware attacks can restrict our travel and affect our food supply chain. It hit home that cybersecurity is national security.

Our adversaries and cyber criminals continue to push limits in cyberspace, creating more national security threats than we have ever seen.

Our adversaries are targeting all levels of U.S. Government, critical infrastructure, industry, academia, private citizens and our allies. This is a shared threat that requires us all to work as a coalition with a common goal. As our National Cyber Director Chris Inglis likes to say, "If you are an adversary, you will need to defeat all of us to defeat one of us."

Nowhere is that more evident than at NSA's Cybersecurity Collaboration Center. In the last year, we opened the door to a new facility where experts from NSA, other U.S. Government agencies and industry partners work side by side outside the NSA fence line to combat cyber intrusions that threaten our nation's military capabilities, intellectual property and technology.

NSA is no longer "No Such Agency," but an open leader in the cybersecurity community facilitating actionable, bidirectional information sharing with more than 100 Defense Industrial Base partners. These efforts align with our partners at the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA), U.S. Cyber Command, FBI, elsewhere in the Department of Defense (DoD) and across many other departments and agencies.

Signals intelligence (SIGINT) is one of our competitive advantages and a primary reason why our partners seek our insights. We can look into foreign space and see what threat actors are doing, including sophisticated nation-state actors. We use that information to inform how we manage our resources and secure our systems, but also to create technical guidance that helps others secure their systems at scale.

Since the standup of NSA's Cybersecurity Directorate in 2019, we've released more than 50 actionable cybersecurity reports. We often collaborate with our U.S. Government and Five Eyes partners to create guidance that stands out from the rest. Our Cybersecurity Advisories have even been implemented in national-level strategies to impose cost on our adversaries.

When our insights are brought into a feedback loop with industry and government partners, amazing outcomes are achieved. We create impact far beyond what any of us can do alone.

I also want to mention our one competitive advantage above all others: Our people. Our success in evolving NSA's cybersecurity mission to meet today and tomorrow's demands is a credit to their expertise and their dedication to securing our nation. Their creativity, persistence and audacity make a difference. That's what truly stands out to me when I read this Year in Review. Thank you to everyone who made this possible.

Regards,



Rob Joyce
Director, NSA Cybersecurity

Responding to National Threats and Priorities

Exposing a Supply Chain Threat

NSA continues to provide partners with unique cybersecurity insights through its foreign signals intelligence (SIGINT) mission. When the cybersecurity firm FireEye – now known as Mandiant – first discovered the highly sophisticated SolarWinds cyber espionage campaign in November 2020, Chief Executive Officer Kevin Mandia and his colleagues made NSA among their first calls.

Mandiant had great insight on what U.S. adversaries and cybercriminals were doing in public space, but wanted to learn what NSA was seeing in SIGINT to build a fuller picture of adversary and cybercriminal activity.



Mandiant representatives, right, chat with Morgan Adamski, NSA Cybersecurity Collaboration Center Chief, during an event at NSA-Washington.

“Piecing those components together can really help paint a picture of not only attribution, but exact tradecraft and what’s occurring during a particular campaign,” said Ron Bushar, Mandiant’s senior vice president and government chief technology officer, during a visit to NSA.

The scale of the SolarWinds cyberespionage campaign highlighted the need for the public and private sector to do more to collaborate. More than 16,000 SolarWinds Orion customers across both sectors were victims of installed malware in the global supply chain compromise.

Early collaboration and information sharing allowed NSA and industry partners to truly understand the scope of the threat and protect the nation’s most sensitive systems. NSA analyzed adversary intent and tradecraft, informed detection and mitigation efforts of U.S. Government and DIB partners, provided cybersecurity guidance and conducted hunt operations. It also shared adversary indicators, behaviors and detection guidance.

On the same day the U.S. Government attributed the campaign to the Russian SVR – also known as APT29 and Cozy Bear – NSA, the FBI and the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA) publicly released a [Cybersecurity Advisory](#) detailing how the SVR was exploiting five publicly known vulnerabilities.

Less than a month later, the National Cyber Security Centre (UK), NSA, FBI and CISA [publicly attributed the SVR to several additional tactics, techniques and procedures \(TTPs\)](#), further degrading their activities by drawing network defenders’ attention to the SVR threat and how to mitigate it.

[NSA’s Cybersecurity Collaboration Center](#) also worked with CISA and industry partners through the Enduring Security Framework (ESF) to reduce the risk of future supply chain compromises.

The partners developed a comprehensive product on how to secure a supply chain by identifying best practices for software suppliers, developers and users.

Countering Ransomware

General Paul M. Nakasone, Commander of U.S. Cyber Command and Director of NSA, declared ransomware a national security threat in 2021 following compromises to U.S. critical infrastructure and key resources. The Colonial Pipeline ransomware attack in May created a fuel shortage on the East Coast and the JBS attack in June briefly halted production on nearly one fifth of the nation's beef, pork and poultry.



Colonial Pipeline fell victim to a ransomware attack in May 2021.

In response, the White House announced a coordinated U.S. Government campaign to counter ransomware. NSA Cybersecurity has played a prominent role by analyzing the threat and sharing insights through its foreign signals intelligence about the cyber criminals profiting from

ransomware and their infrastructure. **NSA has worked closely with U.S. Cyber Command and other government and industry partners to pursue the actors, capabilities and finances fueling this global threat.**

Throughout the effort, NSA ensured that its threat intelligence was disseminated at the lowest possible classification level, so that it generated outcomes.

NSA joined forces with the FBI and CISA to publicly expose cyber actor tactics, techniques and procedures associated with a pair of ransomware variants – [BlackMatter](#) and [Conti](#) – that were being increasingly employed against U.S. organizations, including some that oversee critical infrastructure.

The three U.S. Government agencies also teamed up with the Environmental Protection Agency (EPA) to highlight malicious cyber activity targeting the information technology (IT) and operational technology (OT) networks, systems and devices of U.S. Water and Wastewater Systems (WWS) Sector facilities. Each of these publicly released Cybersecurity Advisories outlined malicious cyber actor activities and provided network defenders with actionable mitigations.

“We saw cyber incidents continually evolve this past year. Today, cybersecurity is national security. We continue to posture ourselves to maintain a competitive advantage as our adversaries persistently attempt to up their game.”

General Paul M. Nakasone, Commander, U.S. Cyber Command, Director, NSA/Chief, CSS



Strategic Competition

Cyberspace has created a setting where cyber adversaries can increase their power, degrade the power of others and gain a strategic advantage – all with a relatively low barrier to entry.

China and Russia continue to conduct persistent malicious cyber campaigns designed to erode democracy, threaten U.S. infrastructure and reduce U.S. economic prosperity. Their TTPs have evolved, enabling them to advance the scope, scale and sophistication of their cyber campaigns.

Part of NSA’s role in characterizing these foreign cyber threats is to provide foundational knowledge for the U.S. Government to defend its networks, which include degrading the capabilities of U.S. adversaries. Two key examples include Joint Cybersecurity Advisories published by NSA, CISA and the FBI:

1. The [“Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments”](#) Joint Cybersecurity Advisory detailed techniques the GRU has used when targeting hundreds of organizations around the world. It also recommended actions defenders can take to make this access method useless, degrading malicious cyber actor capabilities and making it that much more difficult to even begin cyber operations against U.S. networks.
2. The [“Chinese State-Sponsored Cyber Operations: Observed TTPs”](#) Cybersecurity Advisory provided a comprehensive view of how Chinese actors conduct their cyber activities while targeting U.S. and allied networks. The advisory mapped nearly 100 TTPs to the MITRE ATT&CK and D3FEND frameworks which helped network defenders understand the precise mitigation techniques to implement to counter these cyber actors.

Securing COVID-19 Vaccine Data

NSA played a key role in guaranteeing the security of U.S. government efforts to rapidly develop a COVID-19 vaccine through its direct support of Operation Warp Speed. NSA’s experts collected and analyzed data using classified intelligence and indicators of compromise in the cloud hunting operation. **This mission validated that nation-state actors were not able to tamper with the research data related to the safety or effectiveness of the vaccines under development.**

Partnering to Secure Today and Tomorrow

Protecting our Defense Industrial Base

In late 2020, NSA moved into a 36,000-square-foot unclassified Cybersecurity Collaboration Center in an open business park outside NSA's fence line, breaking down barriers between the agency and the outside world. **The NSA Cybersecurity Collaboration Center (CCC) rapidly grew its industry partner base from less than 10 to more than 110 partners in 12 months** by teaming up with Defense Industrial Base (DIB) companies and their cybersecurity service providers that support Department of Defense (DoD) programs for cryptography, weapons and space, and nuclear command and control.

The U.S. military and DIB are still the best in the world, which makes them a top target. This past year, the CCC team worked with industry and interagency partners to reduce the attack surface across the DIB and ensure U.S. sensitive intellectual property, military research, and innovative technical economy are protected at scale in cyberspace.

By sharing actionable, contextualized threat intelligence derived from NSA's foreign signals intelligence (SIGINT) mission, **the CCC engaged in thousands of analytic exchanges** with industry partners and helped identify and prioritize remediation against critical threats. The insights shared by NSA enabled partners to detect adversary targeting of their infrastructure and mitigate the activity to protect their networks and customers. These analytic collaborations successfully occurred across multiple DIB companies and service providers. The results of these interactions are often seen in the blogs, information releases and research published by leading cybersecurity firms.



The NSA Cybersecurity Collaboration Center.



“NSA has unique insights on cyber threats and nation-state actors because of our global signals intelligence mission. Likewise, the private sector has unique capabilities, preeminent research, and intellectual property we need to protect.

We each only see part of the picture. We see something in SIGINT; our partners see activity on their networks. The only way to mitigate the threat is to communicate and collaborate in real-time to drive outcomes.

We don't expect small businesses to defend against nation states alone. Together, we empower a community response.”

*Morgan Adamski, NSA Cybersecurity
Collaboration Center Chief*

Defending the DIB at Scale

While the Cybersecurity Collaboration Center leverages deep insights to disrupt foreign actors attempting to steal critical national security information from DIB networks, it is also providing low-cost, commercial cybersecurity services to scale protection to small and medium-sized businesses for broad impact. **Through the Protective Domain Name System (PDNS) pilot, the CCC has processed more than 3.8B queries and blocked more than 6.5M malicious domains, including known nation-state spear-phishing, botnets and malware.**

To date, the CCC has provided PDNS services to 40 DIB contractors and expects to scale to hundreds more in the coming year. NSA publicly published a Cybersecurity Information Sheet, [“Selecting a Protective DNS Service”](#) and released a [“Cybersecurity Speaker Series”](#) video on PDNS, advising how to implement this low-cost service, which **NSA analysis indicates can block the significant majority of malicious activity.** Visit NSA's YouTube channel to watch the video.

Exposing Vulnerabilities

NSA continues to discover and disclose critical vulnerabilities to private industry. **In 2021, the CCC disclosed a series of critical vulnerabilities in Microsoft Exchange that were patched by Microsoft.** These efforts were timely and important: Microsoft Exchange is used broadly throughout National Security Systems, DoD and DIB networks, and Chinese actors have been conducting widespread exploitation of Microsoft Exchange servers.



NSA Cybersecurity experts can collaborate with industry and government in an unclassified setting at the NSA Cybersecurity Collaboration Center.

Partnering to Extend Impact

The Cybersecurity Collaboration Center (CCC) has also brought NSA closer to interagency partners. Through the Enduring Security Framework (ESF), NSA and the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) worked across sectors to explore cyber threats to 5G. As a result of these efforts and extensive research, a series of five threat-informed papers were publicly published on NSA.gov. The papers are intended to advise network defenders and policymakers on how to secure 5G moving forward:

- [Potential Threat Vectors to 5G Infrastructure](#)
- [Detect and Prevent Lateral Movement in 5G Cloud Infrastructures](#)
- [Securely Isolate Network Resources](#)
- [Data Protection](#)
- [Ensure Integrity of Cloud Infrastructure](#)

In 2021, NSA also began actively participating in CISA's Joint Cyber Defense Collaborative (JCDC), and likewise CISA began participating in the CCC. By doing so, each agency brings its unique expertise and capabilities to the table, driving greater outcomes than either could achieve alone.



Setting the Standards

The CCC consolidated NSA's important work on standards into one home, elevating it and aligning its work with interagency and international partners. These efforts have never been more important, as **foreign adversaries are seeking to use standards bodies as forums to push standards hostile to an open, interoperable, secure and reliant internet. To counter this and ensure a more secure future, NSA authored 15 international standards submissions:** six in secure internet protocols, five in 5G security and four in enterprise IT security. A dozen were accepted; they all spurred greater debate about security issues in the standards.

As commercial products are increasingly relied on to secure National Security Systems, through the National Information Assurance Program (NIAP), the CCC certified 91 commercial components for use in protecting NSS. Additionally, NIAP published 14 Protection Profiles to raise security in those products. Protection Profiles are vendor-agnostic guidelines that raise security in commercial products by defining proper configurations. NIAP continued to strengthen the overall global IT security posture through ongoing partnerships with 30 other nations within the Common Criteria Recognition Arrangement (CCRA). It has positioned the United States as a leader within the global community through further adoption of its standards and by certifying more products than any other nation within the CCRA.

Sharing Timely, Actionable Guidance



“By releasing guidance against tactics and techniques our adversaries are currently using, we empower net defenders to prioritize endless patching and mitigation efforts against the most current threats and raise the cost on our adversaries by exposing their activities.”

Dave Luber, NSA Cybersecurity Deputy Director

Reporting to Secure Systems, Degrade Actor Capabilities

NSA’s public cybersecurity releases exposed malicious adversary activity and provided actionable mitigations that helped net defenders secure their systems. **NSA partnered with one or more U.S. and allied partners on 12 of its 23 reports this past year.** Collaborating on topics relevant across the U.S. Government and private sector enabled NSA and partners to share more comprehensive threat understanding and top defensive actions with a coordinated voice.

Several releases included attribution on active cyber campaigns. By articulating the full threat in a concise manner, these reports helped arm defenders globally to prioritize actions and remove adversary capabilities one at a time. **This work disrupts malicious activities and helps make it more difficult and more costly for any adversary to target U.S. or allied networks.**

Regardless of attribution, NSA continued to detail malicious tactics, techniques and procedures (TTPs) to convey threat knowledge in a uniform manner for public and private organizations to understand and use.

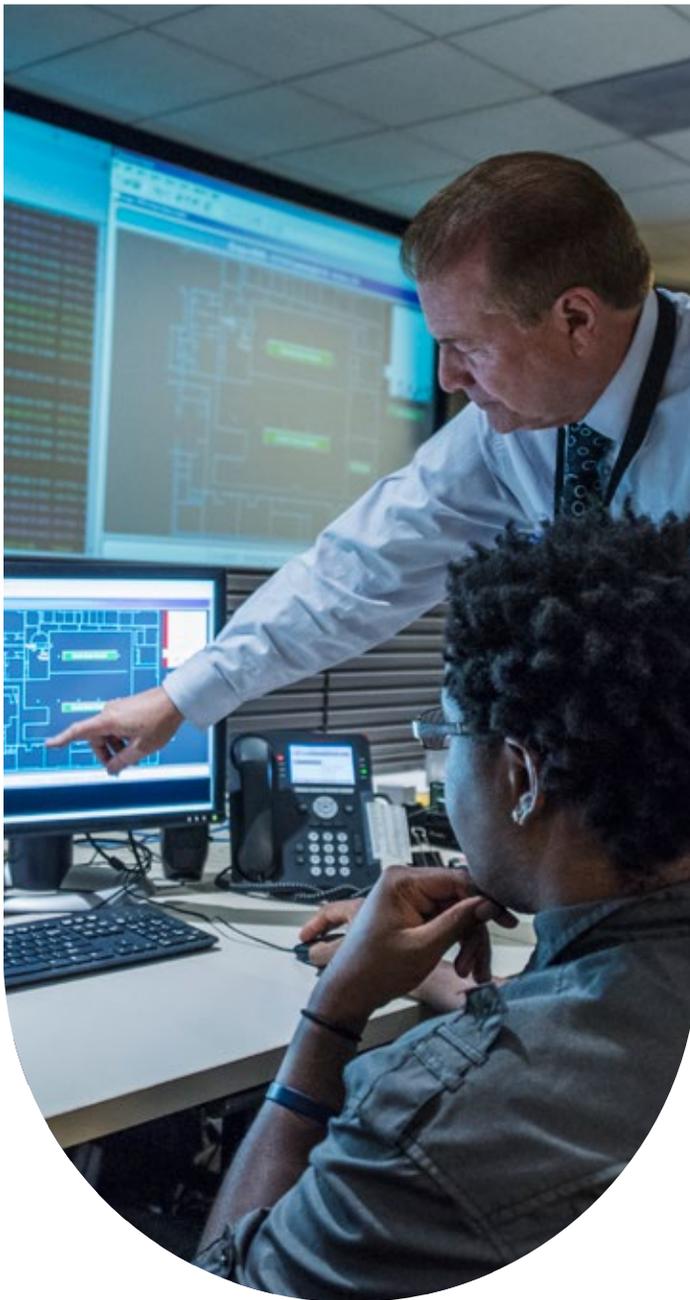
From selecting and securing virtual private networks (VPNs) to safely using the Kubernetes open-source container orchestration system, NSA developed pragmatic, timely preventative guidance. NSA’s experts captured best practices and top recommendations based on real-world experiences. For example:

- [“Selecting and Hardening Remote Access VPN Solutions”](#) highlights key factors when choosing a VPN and implementing configurations – all useful guidance for organizations looking to standardize and mature their telework capabilities and keep sensitive data secure.
- [“Kubernetes® Hardening Guidance”](#) assists organization leaders and network administrators in grasping some of the core security needs when migrating services to a cloud environment and using Kubernetes to manage the virtual, decentralized infrastructure. The guide walks through the architecture, top threats and various security policies and control, along with example configurations to aid those looking to better protect their data and still enjoy the benefits of advancing technologies, such as software containers.

100,000+

The amount of views the “Kubernetes Hardening Guidance” Technical Report received online in the first 24 hours

In the first 24 hours after NSA and MITRE release D3FEND, more than 27K users viewed over 35K pages on d3fend.mitre.org



Creating a Standard Framework

NSA's unique mission makes it challenging to find common language that can be used with government, private sector and commercial partners. **Adoption of a common lexicon enables the sharing of unclassified intelligence products that allow network defenders to execute specific actions to detect or defeat cyber adversaries in the public domain.** NSA Cybersecurity officially adopted the [MITRE Adversarial Tactics, Techniques & Common Knowledge \(ATT&CK\) framework](#) commonly used in the commercial and public sectors this past year to report and characterize observed cyber adversary tactics and techniques.

This has enabled NSA to structure, tag and enrich its cyber threat analysis products, which are now easier to discover and manage – and most importantly – more actionable to partners and customers across the government, private and commercial sectors.

NSA and MITRE also released the complement to ATT&CK: [D3FEND](#). The NSA-funded, MITRE-developed framework provides defensive countermeasures against common offensive cyber techniques.

D3FEND organizes countermeasures and techniques to enable information sharing and operational collaboration, driving more effective design, deployment and better defense of networked systems. This significant body of work captures the complex interplay between threats against computer networks and ways to protect computer networks from cyberattack.

NSA has started incorporating ATT&CK and D3FEND in its public cybersecurity reports. By sharing D3FEND broadly, **NSA and MITRE hope to receive contributions from the cybersecurity community to further refine D3FEND and to promote the adoption of this vocabulary by cybersecurity professionals across government, industry and academia.**

Protecting the Warfighter and Supporting the Combatant Commands



“The Strategic Cybersecurity Program is one example of how we are prioritizing our efforts. We are focusing on specific weapons and space systems because either our threat intelligence indicated they were being targeted or because they are critical to warfighting.”

Brigadier General Lorna Mahlock, NSA Cybersecurity Deputy Director for Combat Support

Evaluating Key Weapons, Space Systems

U.S. Government leaders recognized the threat to key weapons and space systems when creating the Strategic Cybersecurity Program as part of the National Defense Authorization Act for Fiscal Year 2021.

NSA partnered closely with the Department of Defense CIO, Joint Staff, Undersecretary of Defense for Acquisition & Sustainment, and the military services to structure, design and execute the Strategic Cybersecurity Program.

NSA operates the DoD Strategic Cybersecurity Program (SCP) Program Management Office, which oversees the production of cybersecurity scorecards and remediation plans to ensure that critical U.S. weapons and space systems are not vulnerable to cyber adversaries. The plans include both mitigations and monitoring, and cover all warfighting domains – air, land, sea, space and cyber.

NSA successfully worked in concert with the DoD and U.S. military services to assess, prioritize and mitigate vulnerabilities in key capabilities across DoD and are postured to build on those successes in 2022.

NSA also partnered with U.S. Cyber Command and Joint Force Headquarters–Department of Defense Information Networks (JFHQ–DODIN) on efforts to further modernize encryption across U.S. combatant commands. This significantly reduces the chance that U.S. adversaries can access the nation’s most sensitive information.



U.S. weapons and space systems.



Securing Communications

NSA's Commercial Solutions for Classified (CSfC) expanded secure telework capabilities for DoD civilians and service members at the unclassified and secret levels using modern, mobile commercial products, such as mobile phones and laptops. This has been critical to ensuring the health and welfare of the DoD workforce while maintaining mission readiness during the COVID-19 pandemic. **Over the past year, thousands deployed CSfC cybersecurity solutions that provide secure, remote access to National Security Systems (NSS) on classified networks across their enterprise.**

CSfC empowers customers to design and build secure solutions to their needs using NSA's preapproved system designs that cover a variety of communications, including site-to-site connections as well as mobile and tactical telework applications. It has tapped the diversity, speed and agility of commercial markets. In the past year, the National Information Assurance Program (NIAP) added 418 modern, commercial products to the CSfC Approved Components List, significantly expanding CSfC offerings for the DoD workforce.

Strategizing to Secure Nuclear Command, Control and Communications

By preventing and eradicating threats to U.S. Nuclear Command and Control Systems (NCCS) and the National Leadership Command Capability (NLCC), NSA helps ensure command and control of strategic forces and communication between senior leaders.

In 2021, NSA partnered closely with U.S. Strategic Command (USSTRATCOM), which deters strategic attack and employs forces, as directed, to guarantee the security of the U.S. and its allies.

NSA created a Nuclear Command, Control and Communications (NC3) strategy and framework for the USSTRATCOM NC3 Enterprise Center (NEC). The strategy outlines the direction for cyber resiliency and assuring NC3 systems and information. The framework provides an organizational structure for discussing key cybersecurity principles and capabilities required for an assured, reliable and cyber-resilient NC3 enterprise.



U.S. Strategic Command (USSTRATCOM) headquarters.

Supporting the Afghanistan Retrograde

In August, NSA supported the U.S. withdrawal from Afghanistan by providing direct cybersecurity support to operations. The agency also aided efforts to protect tactical and strategic cryptographic equipment and equities.

NSA leveraged the full range of its authorities, expertise and partnerships to provide direct support to the U.S. military, protect operations and improve their cybersecurity posture as they evacuated personnel from the country. NSA Cybersecurity teams provided recommendations to the U.S. military on methods to ensure that its networks were protected against adversary targeting during the withdrawal and provided threat assessments to shape military communications plans.

Within 24 hours of receiving the request, NSA also provided the U.S. military with a one-page visual guide to quickly identify 27 current and commonly fielded forms of high assurance communications security (COMSEC) devices used by the U.S. military and intelligence agencies. It enabled U.S. military and civilian personnel on the ground in Afghanistan to identify, remove and ensure safe disposition during the withdrawal, so that it didn't end up in the wrong hands.



A U.S. Marine carries a child to a plane at Al Udeid Air Base, Qatar.



The 816th Expeditionary Airlift Squadron prepare to load qualified evacuees aboard a U.S. Air Force C-17 Globemaster III at Hamid Karzai International Airport.

Creating Cryptography to Protect Data, Communications



“We build strong cryptography that prevents our adversaries from accessing our nation’s most sensitive systems and data. Our signals intelligence mission, where we break our adversaries’ cryptography, and our many decades of experience provide us with a distinct advantage.”

Neal Ziring, NSA Cybersecurity Technical Director

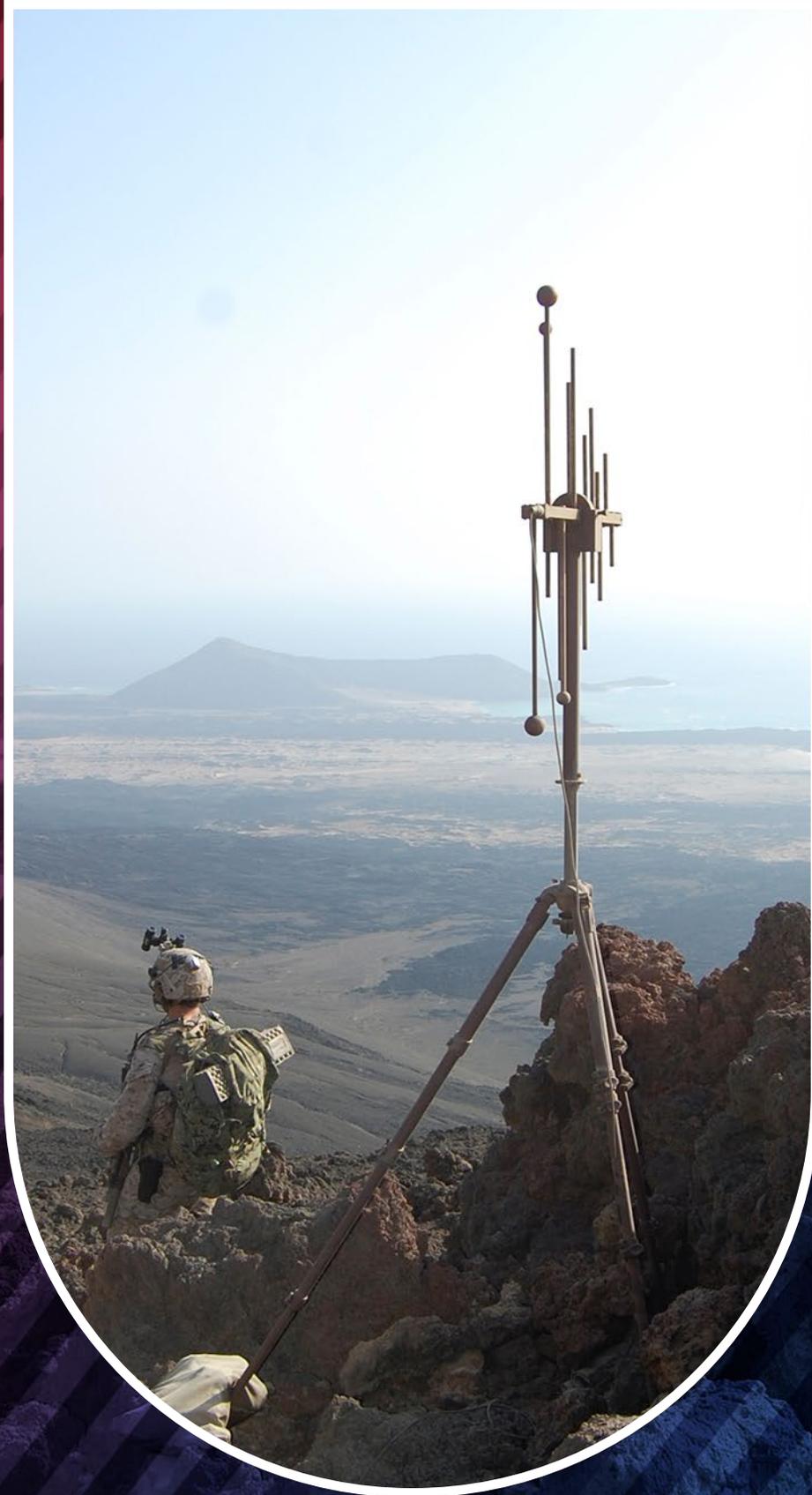
Provisioning Codes, Keys and Cryptographic Solutions

The U.S. Government and U.S. military rely on NSA to produce and distribute the codes, keys and cryptographic materials they use to protect sensitive data from adversary intrusions and protect communications from adversary eavesdropping. This includes the nuclear launch codes and related materials that would be used should the president ever authorize the launch of U.S. nuclear weapons.

145,411

Tamper-indicating products that NSA delivered globally in 2021. These technologies prevent or detect physical exploitation of cryptographic equipment and classified material by adversaries or insiders during shipping or deployment around the world.

NSA provides communications security best practices to ensure secure handling of cryptographic material as well as to secure networks, systems and communications devices used by the Department of Defense to provide command and control, and battlefield awareness.



Cryptographic Modernization

Technology advancements, the theoretical quantum computing threat and escalating adversary aggression have driven NSA's cryptographic modernization efforts for the Department of Defense. A few 2021 modernization successes include:

- For the first time, NSA solely used a modernized key management infrastructure system to more efficiently key the U.S. Air Force F-22 Raptor fleet. The cryptographic devices on all 186 jets secure communications and telemetry.
- NSA, in partnership with the National Reconnaissance Office (NRO), certified the smallest crypto unit ever produced for space applications, enabling cube and small satellites to provide certified, crypto-secured support for the warfighter in a highly contested space environment.
- NSA delivered the first set of updated cryptographic devices to protect National Security Systems (NSS) from potential adversarial quantum computing attacks. While a cryptographically relevant quantum computer remains theoretical, the development and use of one could make key portions of the U.S. cryptographic inventory obsolete.
- NSA is collaborating with foreign partners to develop common key management infrastructure that supports cryptographic interoperability.

In addition to code making, NSA provides technical services and guidance to program managers during the development of cryptographic devices.



The U.S. Air Force relies on NSA Cybersecurity to secure communications and telemetry for its F-22 Raptors.

NSA released a detailed set of frequently asked questions (FAQs) addressing the quantum threat and post-quantum solutions for National Security Systems

[Visit **NSA.gov/cybersecurity/post-quantum-cybersecurity-resources**](https://www.nsa.gov/cybersecurity/post-quantum-cybersecurity-resources)

Defending Critical Systems and Networks



“Information vital to maintaining our security lives on National Security Systems and the nation relies on NSA Cybersecurity to provide the leadership, practices and policies that keep these systems protected from our adversaries.”

Rob Joyce, NSA Cybersecurity Director

Embracing a Zero Trust Model and Mindset

The U.S. Government and the Department of Defense (DoD) continued developing Zero Trust architectures. The Zero Trust model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and continuously looks for anomalous or malicious activity. Leveraging Zero Trust principles enables system administrators to control how users, processes and devices engage with data. These principles can prevent the abuse of compromised user credentials, remote exploitation, or insider threats and even mitigate effects of supply chain compromises.

NSA has been at the forefront of this effort, leading the development of the DoD’s Zero Trust Reference Architecture and the National Security Systems (NSS) Zero Trust Reference Architecture. The Agency established the Zero Trust Working Group within the Committee on National Security Systems to standardize policy and guidance across the NSS community. NSA’s experts also developed an unclassified Zero Trust test bed that enabled collaboration with partners from across the DoD, U.S. Government, industry, academia and foreign partners.



“Embracing a Zero Trust Mindset” is available on YouTube.

NSA publicly released a Cybersecurity Information Sheet on [“Embracing a Zero Trust Model”](#) to outline the concept, benefits and implementation challenges for cybersecurity leaders, enterprise network owners and administrators who are considering embracing the Zero Trust model. It followed up with an [NSA Cybersecurity Collaboration Center Speaker Series video](#) to discuss concepts and dispel common myths and misconceptions.



Defending National Security Systems

In the wake of the SolarWinds global supply chain intrusion and Microsoft Exchange compromise, **NSA played a significant role in the development and implementation of the Executive Order (EO) on Improving the Nation's Cybersecurity.** Signed by the president in May, EO 14028 established that the U.S. Government must lead by example to improve its own efforts to protect against and respond to malicious cyber activity through bold changes and significant investments in cybersecurity. The EO focused on modernizing the cybersecurity defenses of federal networks, improving information sharing between the U.S. government and the private sector on cyber issues and strengthening the United States' ability to respond to incidents when they occur.

NSA led, coordinated and supported several efforts related to the Executive Order, most notably drafting a National Security Memorandum that captures the responsibilities of the National Manager – the NSA Director – in implementing cybersecurity modernization efforts for NSS. NSA held these same network owners accountable for keeping the United States' most sensitive information secure by issuing National Manager Memos that advise network owners to take action to protect against threats and vulnerabilities.

In 2021, NSA developed collaboration forums to share threats, vulnerabilities and mitigations with NSS and critical infrastructure and key resources communities at the unclassified, secret and top secret levels. NSA drew strong attendance from across the Intelligence Community, Department of Defense and federal civilian agencies. **These information exchanges have firmly established NSA's role as a community leader for conversations on NSS threat intelligence and high-priority topics.**



National Security Systems are networks that contain classified information or are otherwise critical to military and intelligence activities.

Protecting Critical Software

In response to EO 14028, NSA coordinated with the National Institute of Standards and Technologies (NIST) to better define critical software, issue security measures for critical software and its associated platforms and create minimal standards for vendors' testing of their source code.

NSA also created an Implementation Plan for National Security Systems to develop processes and workflows for more effective threat sharing, direct mitigations efforts and to capture the current cybersecurity state of NSS.

These efforts culminated in the Office of Management and Budget's memorandum to executive departments and agencies, titled, "Protecting Critical Software Through Enhanced Security Measures," which sets out a phased approach for agency implementation of the NIST guidance.

The Office of Management and Budget followed that memo with another in October, which directs federal departments and agencies to adopt a robust endpoint detection and response (EDR) solution. This will improve the federal government's ability to detect and respond to increasingly sophisticated threat activity on federal networks.

Building a Diverse Workforce That Can Tackle Any Challenge



We have to invest in recruiting and retaining talented people with diverse perspectives because they have the skills necessary to tackle our most complex issues.

Rob Joyce, NSA Cybersecurity Director

Standing for Diversity, Equality and Inclusion

NSA Cybersecurity leaders are committed to building a diverse workforce that reflects the nation in which NSA serves and protects. **It filled critical mission needs and exceeded NSA diversity hiring goals in diversity and disability hires in 2021.** These efforts were facilitated through NSA's relationships with the [National Centers for Academic Excellence in Cybersecurity \(NCAE-C\)](#), including Historically Black Colleges and Universities.

NSA participated in the global #ShareTheMicInCyber campaign this year to amplify African American voices in the cybersecurity community, providing a platform to share their perspectives, stories and accomplishments on a variety of cybersecurity issues and challenges. NSA Cybersecurity Director Rob Joyce handed his official Twitter handle [@NSA_CSDirector](#) – and large following – over to Talya Parker, founder of a non-profit organization designed to increase awareness and diversity in cybersecurity, STEM and private industries. Parker's posts reached 20 countries and 23 million views on Twitter with more than 600 likes.



Rob Joyce's Twitter handle was taken over by Talya Parker for a day.



NSA recommended that students in this year's Codebreaker Challenge download **Ghidra**, NSA's open source reverse engineering tool, to have a leg up on the competition.

Ghidra 10.0, released in 2021, integrates a Dynamic Analysis Framework for the first time, better known as a debugger. This allows users to perform static and dynamic analysis with the same platform.

[Visit Ghidra-sre.org/](https://ghidra-sre.org/)

Promoting and Enhancing Cybersecurity Expertise

U.S. adversaries are constantly improving their capabilities and so must NSA in this era of strategic competition. Cyberspace is an evolving threat environment, forcing its practitioners to learn and adapt or get left behind. Because of this, NSA prioritizes building foundational cybersecurity expertise in its workforce, especially in the areas of security engineering, cryptography and cybersecurity analysis. NSA provides cybersecurity development programs for new employees and those looking to change career paths.

As part of NSA's efforts to continuously develop agile cybersecurity professionals, it promotes higher education and research in cybersecurity. The NCAE-C program, managed by NSA's National Cryptologic School, works with two- and four-year colleges and universities interested in advancing the study of cybersecurity.

NSA and its federal partners, including the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA), the FBI, the National Institute of Standards and Technology (NIST)/National Initiative on Cybersecurity Education (NICE), the National Science Foundation (NSF), the Department of Defense Office of the Chief Information Officer and U.S. Cyber Command combined to execute \$83 million in grants to more than 300 participating schools in the past year.

Attracting the Next Generation of Cyber Warriors

Through programs such as GenCyber and the NSA Codebreaker Challenge, NSA is dedicated to inspiring the cyber warriors of tomorrow:

- **GenCyber:** NSA and the NSF funded 156 K-12 summer cybersecurity camps in 2021 that were used to educate around 3,500 students and more than 800 teachers. Camps were held in 47 states as well the District of Columbia and Puerto Rico. The program strives to be a part of the solution to the nation's shortfall of skilled cybersecurity professionals by increasing awareness for students and teachers about K-12 educational cybersecurity content as well as secondary and career opportunities. The program also aims to increase student diversity in cybersecurity college and career pathways.
- **The NSA Codebreaker Challenge:** Started in 2013, the challenge provides students attending U.S.-based academic institutions the chance to sharpen their cyber skills and get a feel for NSA's critical work to the nation. More than 5,400 students from more than 600 schools participated in 2021's challenge, which focused on a scenario affecting the U.S. Government and critical infrastructure, including the Defense Industrial Base. The tasks involved realistic NSA mission-centric scenarios that tested skills in reverse engineering, computer programming, forensics and vulnerability analysis. Students who perform well in the Codebreaker Challenge are often encouraged to apply to NSA. **Across the country, many colleges and universities have incorporated the Codebreaker Challenge into their curriculums, promoting intercampus engagement which helps strengthen U.S. cybersecurity education nationwide.**



See What NSA's Cybersecurity Expertise Can Do For You

Recommendations for securely implementing:



5G in the cloud



Remote access VPNs to reach data when working anywhere



Protective DNS or encrypted DNS on enterprise networks



Containerized environments with Kubernetes

Mitigations to counter current threats, including:



Global brute force campaigns



Abuse of authentication mechanisms



Ransomware targeting U.S. infrastructure



Malicious cyber activity against operational technology

Find these and more at [NSA.gov/cybersecurity](https://www.nsa.gov/cybersecurity).

