



2023 NSA CYBERSECURITY

{ Year In Review

Welcome

Since World War II, the National Security Agency (NSA) and its predecessors have protected the United States' most sensitive information. As technological advancements have created a more interconnected world with ever-increasing threats, NSA's mission has expanded. NSA has embraced new responsibilities and operational authorities to ensure our networks remain secure.

Today, NSA's cybersecurity mission integrates cryptographic expertise, foreign signals intelligence, vulnerability analysis, defensive operations, and more to prevent and eradicate cyber threats to three key areas.

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 U.S. warfighting capabilities are mission-ready and to 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):** The ever-growing group of companies that design, develop, operate, and maintain the Department of Defense's critical systems, platforms, and technologies required to defend the nation. Their products, services, and capabilities are vital to the security of the U.S. and our allies.

In an effort to be more transparent, NSA publishes an annual year in review sharing information regarding cybersecurity efforts that better equipped U.S. defenses against high priority cyber threats. NSA's efforts to help secure the nation's most sensitive systems **also help your cybersecurity** because NSA cascades these solutions through public guidance and engages with key technology providers to help them bolster the security of their products and services.

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



Top and bottom image courtesy of Getty Images, middle photo courtesy DoD

CONTENTS

02

Letters From
the Director
of NSA & the
Director of NSA
Cybersecurity

06

Vigilance
Toward National
Threat &
Priorities

09

Partnering
with Industry
& Defense
Industrial
Base

17

Arming Net
Defenders with
Guidance

18

Defending our
Most Critical
Networks

21

Modernizing
Cryptographic
Solutions

23

Protecting
the Warfighter &
Supporting
Combatant
Commands

29

Researching
Cybersecurity
Solutions

31

Developing
Current
and Next
Generation
Cyber Experts



Cybersecurity is National Security.

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

A Letter

From the NSA Director

In my role as the Director of the National Security Agency (NSA), I am humbled and privileged to lead a workforce that supports every component of the Intelligence Community and Department of Defense through its signals intelligence and cybersecurity missions.

NSA is the world leader in **making and breaking codes**. Talented people at our Agency work tirelessly to protect our Nation from our foreign adversaries.

NSA's contributions are critical in the current era of **strategic competition**, wherein global powers are competing economically, militarily, technologically and diplomatically.

The People's Republic of China (PRC) has emerged as the pacing challenge to the United States and as a competitor with both the intent and ability to reshape the international order to fit its own designs. The PRC, an adversary that is unique in the scope, scale, and sophistication of the threat it poses, has stated its desire to become one of the world's leading powers.

Russia remains an acute threat and continues to threaten regional security and global stability through its disregard of international norms and its willingness to use its weapons to target civilians and critical infrastructure. We've witnessed a telling example of this during Russia's illegal invasion of Ukraine. Russia has also deployed information operations intended to weaken democratic institutions around the world.

We need to be able to respond to threats from the PRC, Russia, and other global adversaries today and in the future. **We must stay ahead of our global competitors** who constantly seek to reshape the global information environment and the world order as we know it.

Authorities like Section 702 of the Foreign Intelligence Surveillance Act (FISA) allow us to do that. FISA Section 702 is a key foreign intelligence authority that helps keep the United States and its allies safe and secure. Intelligence from Section 702 is used every day to **protect the nation from critical threats, inform U.S. Government strategy, and save American lives**. Since any lapse in this law would have a blinding effect on our insights into hostile foreign actors operating beyond our borders, we look to Congress reauthorizing Section 702.

The authorities with which NSA is entrusted allow NSA to tackle our most significant national security concerns, including **cybersecurity**. Recently, we've seen the nature of conflict evolve: **cyberspace is contested space**. It's become clear that the shift from competition to crisis to conflict can now occur in weeks, days, or even minutes. Every day at NSA, we strive to **prevent and eradicate cyber threats** to U.S. National Security Systems, the Department of Defense, and the Defense Industrial Base (DIB).

The new National Cyber Security Strategy outlines a clear and dedicated focus on leveraging international partnerships to pursue shared goals in securing software, critical infrastructure, and global networks, dismantling and defeating ransomware actors, increasing operational collaboration in cyberspace, and building incident detection and response capabilities.

Our intelligence and cybersecurity relationships with our allies and partners are a strategic asset that will increasingly factor into our competition with our rivals, especially in technological competition.

The global landscape becomes ever more complex as the technology we use in cyberspace continues to advance. One such example is **Artificial Intelligence (AI)**, which has the capacity to upend multiple sectors of society simultaneously. We must stay ahead of our global competitors in the race to understand and harness its potential, as well as protect ourselves from adversarial use. At NSA, we are uniquely positioned to do so by coalescing our deep technical expertise, threat insights, and authorities to support these efforts.

I recently announced that NSA is consolidating its various AI security related activities into a new entity, the NSA Artificial Intelligence Security Center. The AI Security Center, located within our Cybersecurity Collaboration Center, will allow us to work closely across the Intelligence Community, the Department of Defense, the industrial base, national labs, academia, and select foreign partners to **ensure the United States' enduring advantage in AI**.

NSA's principles and values, along with our **culture of compliance and protection of privacy and civil liberties**, have served as the foundation for the cybersecurity successes detailed in this report and will continue to serve as the bedrock of NSA in the future.

At NSA, our people and our partnerships make the difference. NSA employees have a steadfast belief in the importance of the trust granted to them through the oath they swore to uphold. Our deep and enduring partnerships allow us to **tackle threats and scale solutions together to make this Nation - and our allies - more secure**. On behalf of NSA, I share my sincere thanks for the work all of our partners do in this space, since our collective cyber resilience and agile responses to threats are better when we work together.



PAUL M. NAKASONE

General, U.S. Army
Commander, U.S. Cyber Command,
Director, National Security Agency/Chief, Central Security Service

A Letter

From the NSA Cybersecurity Director

The NSA Cybersecurity Directorate was established with the intention of connecting to industry and other partners. That trend continued in the past year, as we leaned into partnerships more than ever before. We focus on taking what we know and turning it into actions that **secure networks and disrupt our adversaries in new ways**. Our domestic and international partnerships help us tackle threats together to **scale cybersecurity solutions** and make even greater impacts.

When we know something, it only provides value when net defenders can take real action with it. By **sharing information bi-directionally in an unclassified environment** with our partners, we improve both cybersecurity and national security.

The **combined talent of our partnerships** is the greatest competitive advantage we have to confront the increasingly sophisticated threats we see today.

In the past year, we've exposed numerous cybersecurity threats. Working with industry and international partners, we identified indicators of compromise associated with a **People's Republic of China (PRC) state-sponsored cyber actor using living off the land techniques -- using built-in network tools to evade defenses without leaving a trace--to target networks across U.S. critical infrastructure**. We benefitted from multiple private sector entities to better understand this threat and released guidance to help network defenders hunt and detect this type of malicious activity on their systems and critical networks.

Working with partner agencies also allowed us to **identify a sophisticated Russian cyberespionage Snake malware tool being used in over 50 countries worldwide**. Together, we attributed Snake operations to a known unit within Center 16 of Russia's Federal Security Service. The technical details we released with partners enabled Federal Bureau of Investigation (FBI) operations and helped many organizations find and shut down the malware globally.

Separately, collaboration with industry partners led to discovering a vulnerability in Citrix servers that could have resulted in information stolen from the Defense Industrial Base. Because of these partnerships, **the zero-day vulnerability was exposed and patched, and the number of vulnerable servers across the country dropped significantly**.

Our Cybersecurity Collaboration Center (CCC) allows us to build coalitions to share information together and address threats like these. This year, the CCC tripled its partnerships, so we now collaborate in more than **750 open and robust relationships** across industry and government, which allows us to scale prevention, detection, and mitigation techniques to **billions of endpoints worldwide**. The CCC

scaled its cybersecurity as a service program to include small-to-medium businesses within the Defense Industrial Base (DIB) supply chain. This year's **400% increase in enrollments in our services** helps to ensure our critical partners in defense – including small and medium-size businesses – don't have to secure their systems alone. Our partnerships allow us to lean forward and proactively share insights as we do what we're charged to do: help secure our Nation's defenses, its most critical networks, and the DIB.

One emerging threat – and opportunity – is Artificial Intelligence (AI). AI and machine learning technologies are being developed and proliferating faster than companies and governments can shape norms, create standards, and ensure positive outcomes. While the tools may enable amazing new defensive capabilities, they may also empower attackers. NSA's recently established **Artificial Intelligence Security Center** within our Cybersecurity Collaboration Center is the Agency's new focal point to apply the unique insights from NSA signals intelligence and technological expertise, while collaborating with industry to help industry counterparts understand, prevent, and mitigate – threats in the AI ecosystem. The center will serve as a focal point to develop best practices, evaluation methodology, and risk frameworks, while we aim to promote secure adoption of AI capabilities.

We also made progress in the marathon to transition to **quantum-resistant cryptography** to protect our networks, the technology we rely on, and our weapons platforms. We completed cryptographic roadmaps for each U.S. combatant command coalition partner to help our partners identify where they need to invest to secure against advanced cyber threats and become fully interoperable with U.S. and allied forces.

In the end, these significant outcomes are powered by the folks at NSA and our partner organizations who innovate, come up with brilliant ideas, and act on them with urgency to secure our Nation and our partners now and in the future.

Regards,



Rob Joyce
Director, NSA Cybersecurity





“

Together, the cybersecurity community is so much better through the power of partnership.

{ Rob Joyce
Director, NSA Cybersecurity



Vigilance

Toward National Threats and Priorities

Countering Global Threats

Together with U.S. and international partners NSA continues to scale its impact against increasing global threats and sophisticated adversaries.

While the U.S. Government relies on NSA's unique foreign signals intelligence insights to inform key decisions, public and private sector collaboration builds on that foundation to better inform understanding of the threats and how to counter them.

Every organization brings their own unique capabilities, authorities, and insights to paint a broader picture – thereby enhancing NSA's ability to prevent and eradicate some of the world's most concerning cyber threats.

Exposing and Mitigating People's Republic of China's Malicious Activity

Together with key industry partners, NSA identified a People's Republic of China (PRC) state-sponsored cyber actor using built-in network tools to target U.S. critical infrastructure. To help network defenders hunt and detect this type of PRC malicious activity on their systems, NSA coordinated with U.S. and international partners to publicly release the ["People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection"](#) joint Cybersecurity Advisory. The advisory provides an overview of hunting guidance and associated best practices, and includes examples of actor's commands and detection signatures.

“

Cyber actors find it easier and more effective to use capabilities already built into critical infrastructure environments. A PRC state-sponsored actor is living off the land, using built-in network tools to evade our defenses and leaving no trace behind, that makes it imperative for us to work together to find and remove the actor from our critical networks.

{ Rob Joyce
Director, NSA Cybersecurity



Hunting Russian Intelligence “Snake” Malware

CYBERSECURITY ADVISORY

In another instance, when an industry partner detected PRC actors targeting critical DIB organizations using a zero-day vulnerability, NSA immediately shared technical indicators with DIB partners to enable discovery on their networks. The vulnerability specifically targeted widely-used devices throughout the DIB so NSA’s daily engagements with industry over a two-month period helped disrupt and mitigate the campaign.

Hunting Russian Intelligence “Snake” Malware


In coordination with partners, NSA identified a sophisticated Russian cyberespionage Snake malware tool being used in over 50 countries worldwide. Together, NSA, USCYBERCOM’s Cyber National Mission Force, FBI, Cybersecurity and Infrastructure Security Agency, the Canadian Cyber Security Centre, the Australian Cyber Security Centre, the New Zealand Government Communications Security Bureau, and the U.K.’s National Cyber Security Centre, attributed Snake operations to a known unit within Center 16 of Russia’s Federal Security Service. This infrastructure was identified across North America, South America, Europe, Africa, Asia, and Australia, including the U.S. and even Russia. The technical detail released with partners helped FBI operations, partnering with many organizations, find and shut down the malware globally.

Collaborating Internationally To Release Guidance

Working across the U.S. Government and international collaborators, NSA has enabled increased sharing through Cybersecurity Advisories regarding nation-state threats.

In a first, we collaborated with the Japan National Police Agency and the Japan Center of Incident Readiness and Strategy for Cybersecurity, NSA alongside the FBI and the U.S. Cybersecurity and Infrastructure Security Agency (CISA), released a joint Cybersecurity Advisory to detail activity of PRC-linked cyber actors known as BlackTech. BlackTech demonstrated capabilities in modifying router firmware without detection and exploiting routers’ domain-trust relationships for pivoting from international subsidiaries to their parent companies in Japan and the U.S.

In another first, NSA worked with the Republic of Korea’s National Intelligence Service, National Police Agency, and Ministry of Foreign Affairs along with our partners at the FBI, and U.S. Department of State, to jointly issue a Cybersecurity Advisory highlighting the use of social engineering by Democratic People’s Republic of Korea state-sponsored cyber actors to enable computer network exploitation globally against individuals employed by research centers and think tanks, academic institutions, and news media organizations.



The Department of Defense (DoD) serves as the Sector Risk Management Agency for the Defense Industrial Base (DIB). In this role, the Department interfaces with DIB companies, monitors and prioritizes threats, oversees incident management, and provides technical assistance, among other duties. The Department's DIB cybersecurity initiatives include the DIB Cybersecurity Program, the DoD Cyber Crime Center's DoD-DIB Collaborative Information Sharing Environment, National Security Agency's Cybersecurity Collaboration Center, and the Enduring Security Framework.

Excerpt from the DoD Cyber Strategy Summary
released September 2023

Partnering

With Industry and Defending the Defense Industrial Base

Protecting the Defense Industrial Base (DIB)

Although many people associate the DIB with large defense contractors, more than 70% of the DIB is made up of small businesses. Upon signing a contract with DoD, these companies often become targets for nation state actors. Small businesses generally do not have the resources to defend against nation-state activity alone. NSA works with DIB companies large and small — NSA's critical partners in defense - bringing the world's leading code-making and code-breaking Agency to stand by their side.



We are at the forefront of change to share our insights with the private sector. We see the power of NSA's expertise in a way we haven't seen before.

{ Morgan Adamski
Chief, Cybersecurity Collaboration Center

NSA provides no-cost cybersecurity services to DoD contractors, informed by NSA's decades of expertise in making and breaking codes. These services are designed to defend against the top ways NSA sees foreign adversaries targeting the DIB and are infused with NSA's unique insights and analytics. In 2023, thanks to aggressive outreach and development efforts, **NSA grew cybersecurity service enrollment by almost 400%**. NSA now provides cybersecurity assistance to more than 600 companies within the DoD supply chain, including suppliers who may lack adequate cybersecurity resources of their own.

While these services are open to any company with an active DoD prime contract or subcontract, NSA launched several new campaigns in 2023 to prioritize outreach to companies supporting:

1. The U.S. Indo-Pacific Command Area of Responsibility
2. The Russia/Ukraine conflict, and
3. DoD's priority weapons systems

Further, NSA worked with DoD's Office of Small Business to **ensure minority-owned small businesses are aware of these services** and have the opportunity to leverage them for cost savings and better network security.

What NSA's Industry Partners Are Saying:

"As a small business, we don't have the unlimited resources that the big players have, so we appreciate anything that gives us an edge. It is one less thing to think about, one less expense, and one less worry."

The Enduring Security Framework (ESF), through collaboration with 17 government and 62 industry partners, released 6 security products addressing threats within the Communications, DIB, and Information Technology critical infrastructure sectors. Specifically, ESF's products addressed threats associated with 5G, identity and access management, and the software supply chain. These issuances provided impactful recommendations, and established industry best practices to mitigate the identified threats.

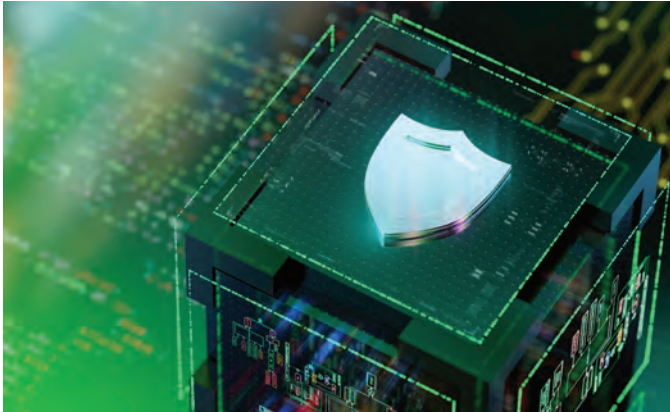


Photo courtesy of Getty Images

- Securing the Software Supply Chain: Recommended Practices Guide for Suppliers
- Securing the Software Supply Chain: Recommended Practice Guide for Customers
- Potential Threats to 5G Network Slicing
- Recommended Best Practices for Administrators – Identity and Access Management
 - » Identity and Access Management Educational Aid & associated talking points
- 5G Network Slicing: Security Considerations for Design, Deployment, and Maintenance

Scaling DIB Cybersecurity Services

This year, NSA also enriched its offerings by harnessing NSA's unique insights on nation-state cyber activity. NSA's Protective Domain Name System (PDNS) service, which blocks users from connecting to known malicious or suspicious websites, is a prime example. NSA developed a custom threat feed for PDNS through which **NSA is providing hundreds of unique Indicators of Compromise (IOCs) per week** to its DNS filtering vendor so they can update their blocklist. These IOCs are derived from three sources:

1. NSA's SIGINT insights,
2. NSA analytics, or
3. Tipped from inter-agency, industry, or international partners.

To date, NSA's PDNS service has generated **10 billion blocks for participating customers**. Of these, 20 million blocks have come from NSA-provided indicators, meaning **NSA is thwarting emerging malicious cyber activity which would have otherwise gone undetected and unmitigated**. These IOCs are also being shared across the U.S. Government and international partners to enable defensive actions.

This year, NSA also improved its **vulnerability scanning program to offer comprehensive attack surface management support**. This program offers two significant benefits for DIB businesses. First, it leverages open source tools to provide companies with a full inventory of their internet-facing assets, since **you can't protect what you don't know about**. Then, this program runs vulnerability scans across those assets and provides a tailored report

with vulnerabilities prioritized leveraging NSA's insights about what nation-state actors are exploiting.

New this year, NSA also launched a "continuous monitoring" feature. Every day, NSA monitors various sources to see when nation-state actors begin exploiting publicly known vulnerabilities. When a vulnerability goes from "known" to "exploited," NSA immediately searches its asset discovery inventory to identify which DIB customers may have that vulnerability within their environment, and flag for them that there is active exploitation against a device that is present within their environment. These notices have an 80% response rate and prove that as a result, **companies are finding and fixing issues prior to compromise and data exfiltration**.

This year, the attack surface management program helped **uncover a massive, People's Republic of China-associated campaign targeting multiple DIB companies by leveraging a vulnerability in Citrix environments**. As a result of NSA's collaboration with large and small DIB companies and Cisco, NSA publicly exposed this campaign in conjunction with a patch release. Independent researchers published blogs noting that within days of the advisory's publication, the number of vulnerable servers across the U.S. and allied nations dropped by almost 25%.

NSA's **threat intelligence collaboration service** matured this year. Through this service, companies can receive non-public, DIB-specific NSA threat intelligence through a secure, unclassified collaboration channel. This method gives companies access to NSA's analytic capabilities simply by opening an app on their phone, increasing their capacity and ability to take action and better protect their- and their customer's-networks.


Increasing Innovative Pilots


Investment in DIB cybersecurity services didn't stop there. NSA launched four new pilots this year, which will run for 12 months and will measure if the service is effective at mitigating nation-state activity, low-cost, and scalable with no significant overhead to participating companies. The new pilots are:

- **Cloud Security:** As cloud computing is swiftly becoming the norm for cybersecurity, NSA is focusing efforts on discovering and mitigating vulnerabilities and misconfigurations within the DIB that leave their networks and intellectual property vulnerable. This pilot will also provide NSA CCC analysts with the data necessary to understand the DIB cloud attack surface, which will be used to craft and distribute DIB-specific cloud security guidance.
- **Threat Hunting:** Identifying and mitigating threats before they cause harm involves actively providing a system information and event management platform to DIB partners to facilitate the detection and mitigation of malicious and suspicious network activity. NSA analysts will hunt alongside the DIB partners and will develop threat-hunting guides and analytics to distribute throughout the DIB.
- **Phishing Protection:** Phishing attacks are pervasive. This pilot provides DIB customers with a secure email gateway to filter phishing attacks, along with access to a sandbox to better understand any malware associated with the malicious attachments to enable appropriate mitigation development.
- **Autonomous Penetration Testing:** This pilot innovatively leverages automated tools, algorithms, and AI to identify digital vulnerabilities more continuously than human capabilities. Mimicking the actions of hackers, this testing provides real-time threat assessments to reduce human intervention, increasing efficiency and providing a more insightful view into how our adversaries are thinking.

By the Numbers

750 
Partners

10B 
Malicious/suspicious domains blocked, including ransomware activity and nation-state malware, spearphishing, and botnets

100s 
Of new unique IOCs fed into NSA's blocklist weekly

20M 
Blocks generated from NSA's unique IOCs

312,000 
Internet-facing assets identified and inventoried for participating DIB companies

1.3M 
Vulnerabilities discovered and flagged for remediation

550+ 
Partner Vulnerability Notifications sent, with 80% response rate

70 
Unique clusters of known nation-state activity consistently tracked by NSA and industry

Multiple 
Nation-state campaigns targeting DIB revealed, including those leveraging zero-day vulnerabilities

Securing Artificial Intelligence (AI)

NSA's new AI Security Center, housed at the Cybersecurity Collaboration Center will promote the **secure development, integration, and adoption of AI capabilities** within national security systems and the DIB. This center will also leverage NSA's unique foreign signals intelligence insights to help industry understand how adversaries use and target AI. By engaging leaders from U.S. industry, national labs, academia, in concert with the Intelligence Community, the DoD, and foreign partners, the AI Security Center will help develop AI security best practices and guidance.

Partnering to Tackle Threats and Establish Standard

The Center for Cyber Security Standards (CCSS) is focused on authoring, informing, and driving adoption of standards for telecommunications, with a focus on securing 5G and preparing protocols for quantum-resistant cryptography. To date, CCSS has authored and submitted more than **95 standards for 5G, cloud networks, and internet protocols. This work ensures security is baked in and reduces our adversaries' ability to steal U.S. intellectual property.** NSA engages in more than 15 Standards Development Organizations and more than 40 working groups. NSA supported the U.S. Government by providing technical expertise in various forums. At the International Telecommunication Union Telecommunication Sector forum, CCSS served as the acting U.S. delegation working in close partnership with Department of State. CCSS advanced multiple secure protocol standards drafts at the Internet Engineering Task Force, to ensure post-quantum resistance and interoperability.

NSA's CCSS is now a member of the Open Radio Access Network (O-RAN) Alliance, an international consortium that develops Radio Access Network (RAN) standards for 5G. The O-RAN Alliance has been historically closed to U.S. Government participation and formerly more focused on market incentives than security requirements. With RAN technology at the core of 5G infrastructure, participation in the consensus-driven O-RAN Alliance represents a way for the U.S. to **bolster security objectives for 5G.**

Through the Enduring Security Framework, CCSS completed a study to reinvigorate U.S. and allied investment in Standards Development Organizations (SDOs), which ensured the long-term security of critical technologies. The group assessed technical and geopolitical threats to international SDOs and developed strategies to counter these threats. NSA and its U.S. Government, industry and international partners increased awareness about the threats to standards

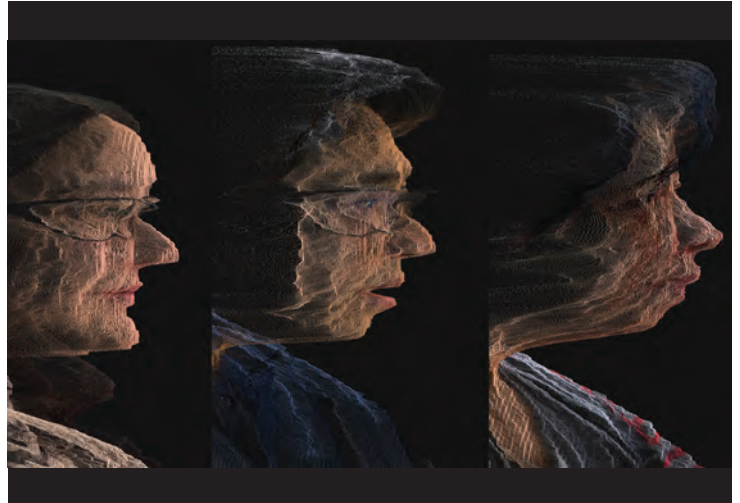


Photo courtesy of Getty Images

and strategized to combat these threats. **The greatest way to combat foreign adversarial influence in international SDOs is for nations that share the same values of security, privacy, and global market competition to contribute technically sound standards proposals.**

Commercial products are increasingly relied upon to secure National Security Systems (NSS). Through the National Information Assurance Program (NIAP), the CCC **certified 57 commercial components for protecting NSS.** Additionally, NIAP published 3 Protection Profiles to raise security in those products. Protection Profiles are vendor-agnostic guidelines that raise security in commercial products by defining minimum security and testing requirements. NIAP is also ramping up to update Protection Profiles to be compliant with Commercial National Security Algorithm (CNSA) 2.0 guidelines, multifactor authentication and Zero Trust principles.

NIAP continued to strengthen the global IT security posture through ongoing partnerships with 31 nations within the Common Criteria Recognition Arrangement (CCRA). The CCRA guarantees consistent evaluations between members and mutual recognition to allow vendors to test once and then sell in multiple countries. 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. NIAP continued to chair the CCRA Management Committee and orchestrated collaboration towards mutual recognition. NIAP also hosted the International Common Criteria Conference and the Common Criteria Meeting at Washington, D.C. with 26 countries represented, further emphasizing the **value of international partnerships for the next generation of commercial technologies.**



Image taken during the Threats to Standards Summit.

NSA hosted a Deception Operations working group with industry partners. This working group developed from industry partner success with the use of honeypots and a desire among our partners to share other tools and techniques associated with deception operations. Industry partners shared their experiences and explained various approaches to deception operations while NSA subject matter experts offered their technical perspectives. The working group created an open dialogue for future collaboration between industry and NSA to explore new techniques to not only defend networks against foreign adversaries but also learn more about the evolving techniques malicious actors are using to target the Defense Industrial Base, DoD, and other U.S. critical infrastructure.

NSA also continued to engage with partners to establish cybersecurity standards by hosting the inaugural “Threats to Standards” Summit, bringing together standards experts across the U.S. government, foreign partners, industry, and academia to explore growing challenges and risks associated with cybersecurity standards.



“

What this collective effort has accomplished already is the creation of a road-map for our partners to provide accountability and help us all continue to improve.

↳ Morgan Adamski
Chief, Cybersecurity Collaboration Center

NATIONAL SECURITY AGENCY CYBERSECURITY SERVICES



Drive Down Risk, Protect DoD Information

NSA is offering companies with an active DoD contract (sub or prime), or with access to non-public, DoD information, several threat-informed cybersecurity solutions to help reduce risk of network compromise and protect sensitive but unclassified information.

Benefits



Receive NSA Threat Intel

Partner with NSA on non-public, DIB-specific NSA threat intelligence



Improve Network Defense

Our services will help increase the security of your networks



Attain Mitigation Guidance

We provide guidance to mitigate the vulnerabilities illuminated using our services



Engage Privately

All partnerships are underpinned by Non-Disclosure Agreements (NDAs)



CMMC Support

Our services support several NIST 800-171 requirements for Risk Assessment, System and Communications Protection, and System and Information Integrity families of requirements.

Success By the Numbers

- Blocked **1B** instances of known malicious or suspicious cyber activity through Protective DNS
- Identified **over a million** network vulnerabilities for remediation
- Discovered **over 8,000** vulnerable host devices
- Identified **over 202,000** vulnerable Partner IPs
- Identified **almost 70,000** vulnerable connective services

OUR SERVICES



Protective Domain Name System (PDNS)

Block users from connecting to malicious or suspicious domains, driving down risk and protecting DOD information.

10B Malicious/suspicious domains blocked, including nation-state spear phishing, malware, botnets, and ransomware activity.

CMMC Support - NIST 800-171 System & Information Integrity 3.14.06



Attack Surface Management

Find and fix issues before they become compromises.

Step one: identify internet-facing assets and determine possible vulnerabilities. Step two: company receives a tailored remediation list, prioritized by severity and likeliness of exploitation based on NSA's unique insights.

CMMC Support - NIST 800-171 Risk Assessment 3.11.02, 3.11.03



Threat Intelligence Collaboration

Partner with NSA to receive non-public, DIB-specific threat intelligence and the opportunity to engage on the materials being shared.

Our services have illuminated, exposed, and remediated active nation-state exploitation attempts across hundreds of enrolled customers.

CMMC Support - NIST 800-171 System & Information Integrity 3.14.03

Enrollment is Easy:

1. Click "GET STARTED" on nsa.gov/ccs
2. Confirm you meet eligibility criteria
3. Sign DIB Framework agreement

Ask us about additional pilots and services!

Industry Partner Testimonial:

“ Thank you for your support during the seamless integration of the NSA Cyber Security suite for the Defense Industrial Base... Within fifteen minutes... we were able to configure our... firewall for the various services.”





Arming

Net Defenders with Guidance

Sharing Timely, Actionable Guidance

Net defenders have a lot on their plates in today's sophisticated threat landscape, and they need timely information to mitigate against significant vulnerabilities and protect their networks against cybercriminal and adversary threats.

NSA's public reports, often released with increasingly more collaborators, help arm net defenders with the guidance they need to address these critical cybersecurity issues.

In coordination with collaborators, NSA produced 27 Cybersecurity Advisories and Cybersecurity Information Sheets for public release this year. Available on NSA.gov, these reports cover a wide array of topics from how to best secure home networks, to how the North Korean government uses social engineering to hack think tanks, academia, and the media.

Another example helps organizations **contextualize deepfake threats**. Deepfakes are AI-generated, highly realistic synthetic media that can be abused to threaten an organization's brand, impersonate leaders, and enable access to networks, communications, and sensitive information. In collaboration with the FBI and CISA, NSA released the "Contextualizing Deepfake Threats to Organizations" cybersecurity information sheet. This offered an overview of synthetic media threats, techniques, and trends, as well as recommendations, guidance and mitigation strategies focused on protecting organizations from evolving deepfake threats.

By publishing this guidance publicly, NSA along with the co-authoring agencies are able to provide important mitigation steps to help protect a range of network information systems.

NSA also streamlined the release of indicators of compromise associated with various types of malware through automated Network Defense Notice (NDN) reporting. These NDNs provide community partners with quick updates on indicators of compromise related to malware observed in the wild that **they can use to prevent potential compromises of their systems**.

27

Cybersecurity Advisories
& Cybersecurity Information Sheets
For Public Release

Defending

Our Most Critical Networks

Defending Key Systems

NSA continues to support implementation of the “Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems”, known as National Security Memorandum-8 (NSM-8).

This memo provided the NSA Director, as the National Manager for National Security Systems (NSS), new authorities that increased NSA’s cybersecurity visibility into networks that contain classified information or are otherwise critical to military and intelligence activities across the Government. Since NSM-8 was signed, NSA has even closer relationships with the more than 50 U.S. departments and agencies that own or operate NSS. NSA continues to increase the security of critical U.S. Government systems to protect sensitive military and intelligence data from our adversaries.

Protecting The Nation’s Secrets

NSA is integrated into the design and build of DoD’s national security and weapons systems and their cryptography. NSA continues to **secure millions of devices around the world** and manage the infrastructure to key those devices through its keys, codes, and cryptography mission. This includes **producing and distributing the keys, codes, and cryptographic materials that the U.S. Government and military use** to secure weapons, satellites, communications, and many other systems in which national security critically relies.

NSA is responsible for protecting the nation’s most critical secrets from the nation’s most capable adversaries, the cyber-capable nation-states and individuals who want to get into our networks or attack our encryption.

NSA’s keys, codes and cryptography secures everything from NSA-certified tactical radios and any encrypted gear in the hands of U.S. soldiers, sailors, airmen, guardians and marines to their critical weapons platforms, including nuclear command and control systems. NSA **ensures these systems our warfighters are using are resilient to cybersecurity attacks** and protect the US strategic advantage in conflict.

Within the past year, NSA’s unclassified **analysis of PRC obfuscation infrastructure yielded better defense of national security systems**. The Cybersecurity Collaboration Center identified malicious cyber activity attributed to the PRC through analytic tradecraft using unclassified commercial threat intelligence data feeds. Automated generation of sensor fingerprints based on this tradecraft streamlined identification of the PRC activity against national security systems network fabric.

Securing Operational Technology

Cyber actors are willing to conduct malicious cyber activity against critical infrastructure by exploiting internet-accessible and vulnerable Operational Technology (OT) assets. NSA evaluated numerous DoD sites, released multiple Cybersecurity Advisories and Network Defense Notifications to secure OT, and continues to secure OT infrastructure and national security systems. To that end, NSA released a repository for OT intrusion detection signatures and analytics to the NSA CyberGitHub. The capability, known as ELITEWOLF, can enable defenders of critical infrastructure, the Defense Industrial Base, and national security systems to identify and detect potentially malicious cyber activity in their OT environments.

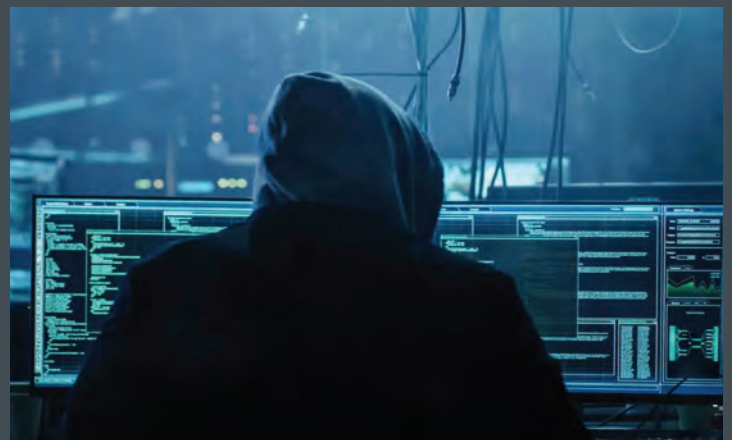


Photo courtesy of Getty Images

NSA CYBERSECURITY REPORTS

UNIQUE. TIMELY. ACTIONABLE.

NSA's guidance notifies network defenders of relevant threats and explains how to protect their systems by detecting and mitigating the malicious activity.

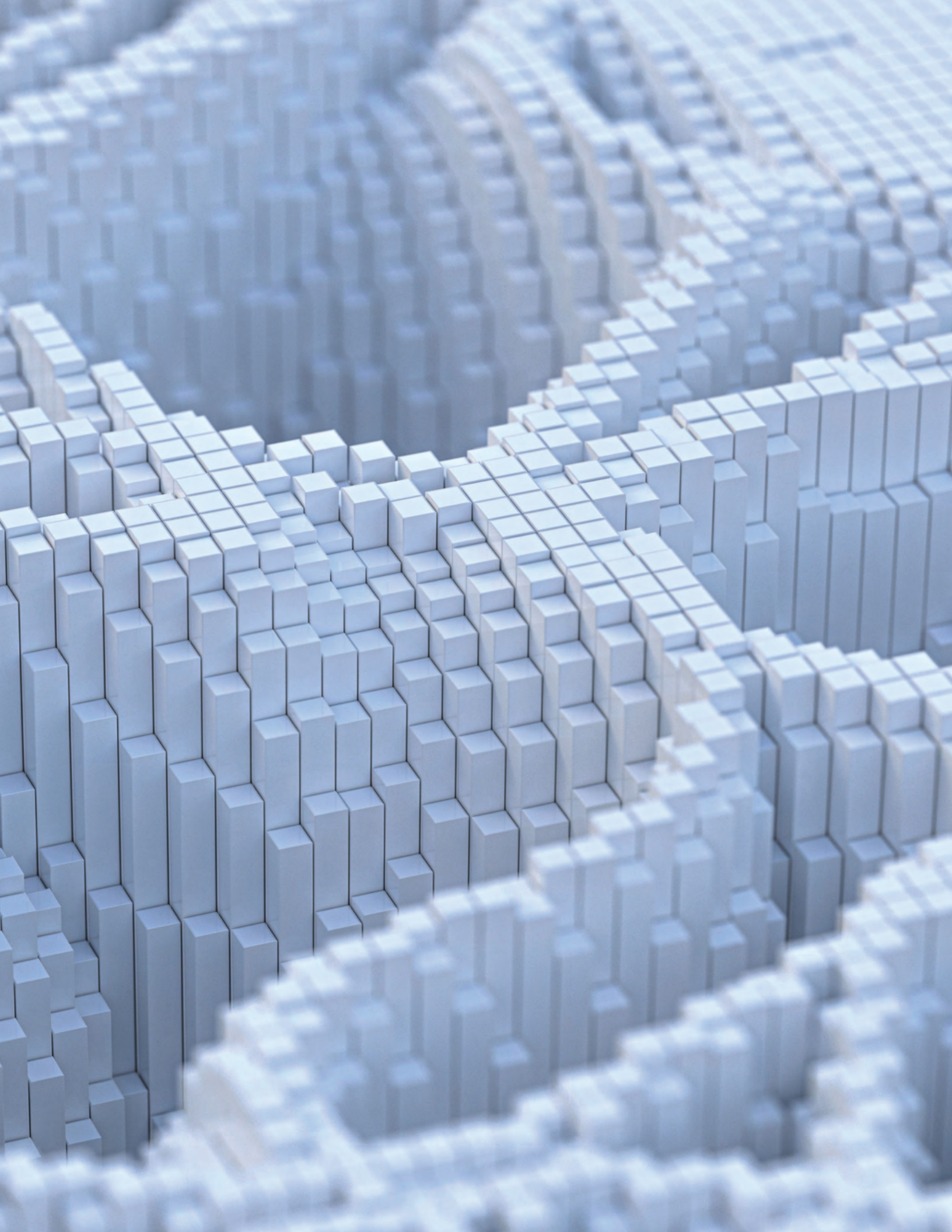
NSA collaborates with government and industry partners to develop and share a comprehensive understanding of nation-state and cybercriminal malicious activity.

NSA and its partners also work together to recommend proven defensive measures that can prevent and even eradicate cyber threats.



Visit [NSA.gov/cybersecurity-guidance](https://www.nsa.gov/cybersecurity-guidance) to review NSA's cybersecurity advisories and technical guidance.

Receive the latest alerts by following @NSACyber on X.



Modernizing

Cryptographic Solutions to Protect Data and Communications

Progressing Toward Quantum-Resistant Cryptography

When achieved, a cryptanalytically relevant quantum computer will change the game. It will introduce threats to our nation's most critical information systems and will break cryptographic systems that secure the internet and information systems worldwide.

Quantum-resistant cryptography continues to be the best defense against this looming threat.

NSA continues to strategically execute National Security **Memorandum-10 (NSM-10)**, "Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," which directs U.S. Government agencies to migrate vulnerable cryptographic systems to quantum-resistant cryptography, a multi-year transition.

As the National Manager for National Security Systems (NSS), the NSA Director oversees the transition to quantum-resistant cryptography across the more than 50 government departments and agencies that use NSS.

Continued partnerships and collaboration with government and private partners is key to fighting this cybersecurity challenge. NSA partners with the National Institute of Standards and Technology (NIST) — the U.S. Government commercial algorithm approval lead— as well as the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence Science and Technology (ODNI S&T), the DoD, and external standards organizations.

The cybersecurity community - including industry, government, and academia - must plan now to modernize cryptography. Quantum computing may not feel like an imminent threat, but it is a looming threat for which action must be taken now.

In the past year, NSA built upon its previously published Commercial National Algorithm Suite 2.0 that notified NSS owners, operators, and vendors of the future requirements for quantum-resistant algorithms for use in all NSS. In March and June, NSA released guidance to assist the U.S. Government to identify and inventory quantum-

vulnerable cryptography, strengthen the current set of cryptography, and **plan for migration to quantum resistant cryptography**. Transitioning toward this modernization includes inventorying cryptography and prioritizing, scheduling, and applying resources toward quantum-resistant efforts, as well as planning to adopt NSA's quantum-resistant algorithm suite and NSS and NIST's cryptographic standards.



Post-quantum cryptography is about proactively developing and building capabilities to secure critical information and systems from being compromised through the use of quantum computers. The transition to a secured quantum computing era is a long-term intensive community effort that requires extensive collaboration between government and industry. The key is to be on this journey today and not wait until the last minute.

{ Rob Joyce,
Director of NSA Cybersecurity

The transition to quantum-resistant cryptography is just one example of how NSA is staying a step ahead of our nation's adversaries to protect our most sensitive data. NSA continually modernizes its cybersecurity solutions to be agile, threat adaptive, and scalable across multi-domain operations.



U.S. Navy photo by Mass Communications Specialist
3rd Class Nicholas V. Huyhn

Protecting

The Warfighter and Supporting Combatant Commands

Supporting the Military

As part of the DoD, NSA is a combat support agency and supports the military services by providing two key missions: foreign signals intelligence and cybersecurity. While NSA's foreign signals intelligence experts deliver intelligence support to military operations, its cybersecurity experts help ensure military communications and data remain secure.

NSA furthered its robust partnership with U.S. Cyber Command, providing support to **hunt forward operations** wherein teams deploy around the world at the request of our partners to assist them against malicious cyber actors.

Warfighters must have confidence in their operations. NSA's contributions help to do just that, so that the U.S. military has the ability to secure communications for operations such as nuclear command and control and differentiate between friend and foe. Together with government partners, NSA helps ensure key management functions, networks, systems and communications devices used by the DoD are secure. NSA also delivers communications security best practices to ensure that the cryptographic material used with these systems and devices is securely handled.

NSA also provides cryptographic security products to meet unplanned emergent requirements and to support urgent missions. In the last year, NSA rapidly deployed approximately **550 communications security (COMSEC) devices** to support mission operations during global crises, and **delivered 234,415 tamper-indicating products** globally in 2023. The tamper-indicating products prevent or detect physical exploitation of cryptographic equipment and classified material during shipping or deployment around the world.

In the last year, NSA continued to **support 61 unique customers for critical operations** such as U.S. Indo-Pacific Command, U.S. European Command, the Joint Chiefs of Staff, U.S. Transportation Command, National Aeronautics and Space Administration (NASA), Federal Emergency Management Agency (FEMA), and many more.

NSA participated in **more than 20 cyber table top exercises and technical exchange meetings** which resulted in 7 vulnerability assessment reports with mitigation plans and engineering security recommendations. NSA continues to help provide guidance to develop defensive monitoring strategies to help improve the situational awareness of weapons platforms.

NSA also partnered with the Space Development Agency (SDA) to develop the Proliferated Warfighting Space Architecture that allowed the SDA to successfully launch their first ten satellites, marking a new era in national defense.

550

COMSEC Devices
Rapidly Deployed

234,415

Tamper-indicating
Products Delivered
Globally

61

Unique Customers
Supported for Critical
Operations

20+

Cyber Table Top
Exercises & Technical
Exchange Meetings



In addition, NSA participated in multiple briefings and discussions with U.S. Space Command leadership and staff. NSA provided insights to members of U.S. Space Command staff regarding cybersecurity service offerings and business practices used by the Cybersecurity Collaboration Center to initiate and develop relationships with industry partners. U.S. Space Command participants also offered a brief regarding U.S. Space Command's commercial relationship development. This partnership will help facilitate further expansion of the Cybersecurity Collaboration Center's partnerships among key U.S. Space Command partners.

As previously described, the entire cybersecurity community must plan now to modernize encryption and prevent against the looming quantum threat. In the past year, NSA continued its efforts to **modernize encryption across the U.S. combatant commands**. By working with U.S. Cyber Command and Joint Force Headquarters-Department of Defense Information Networks, NSA is reducing the chance that U.S. adversaries can access warfighter communications and sensitive data.

The Joint COMSEC Monitoring Activity (JCMSA) continued to identify the leakage of critical military operation details and VIP travel information found in unclassified communications that can increase risks to missions and personnel. JCMSA issued reports to Combatant Commands for action and remediation related to these findings.

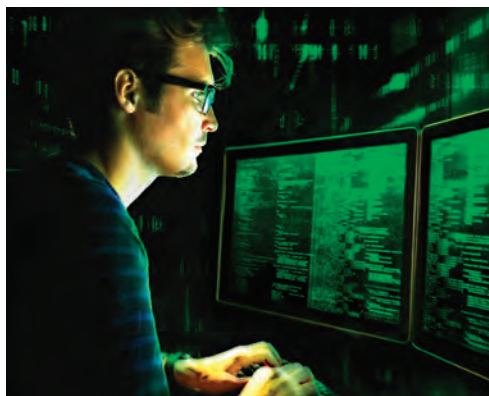
Assessing Systems and Creating Roadmaps

Conducting critical **cybersecurity assessments on some of the nation's most important weapons and space systems** across all warfighting domains helps ensure they aren't vulnerable to cyber adversaries. NSA continued this critical work over the past year.

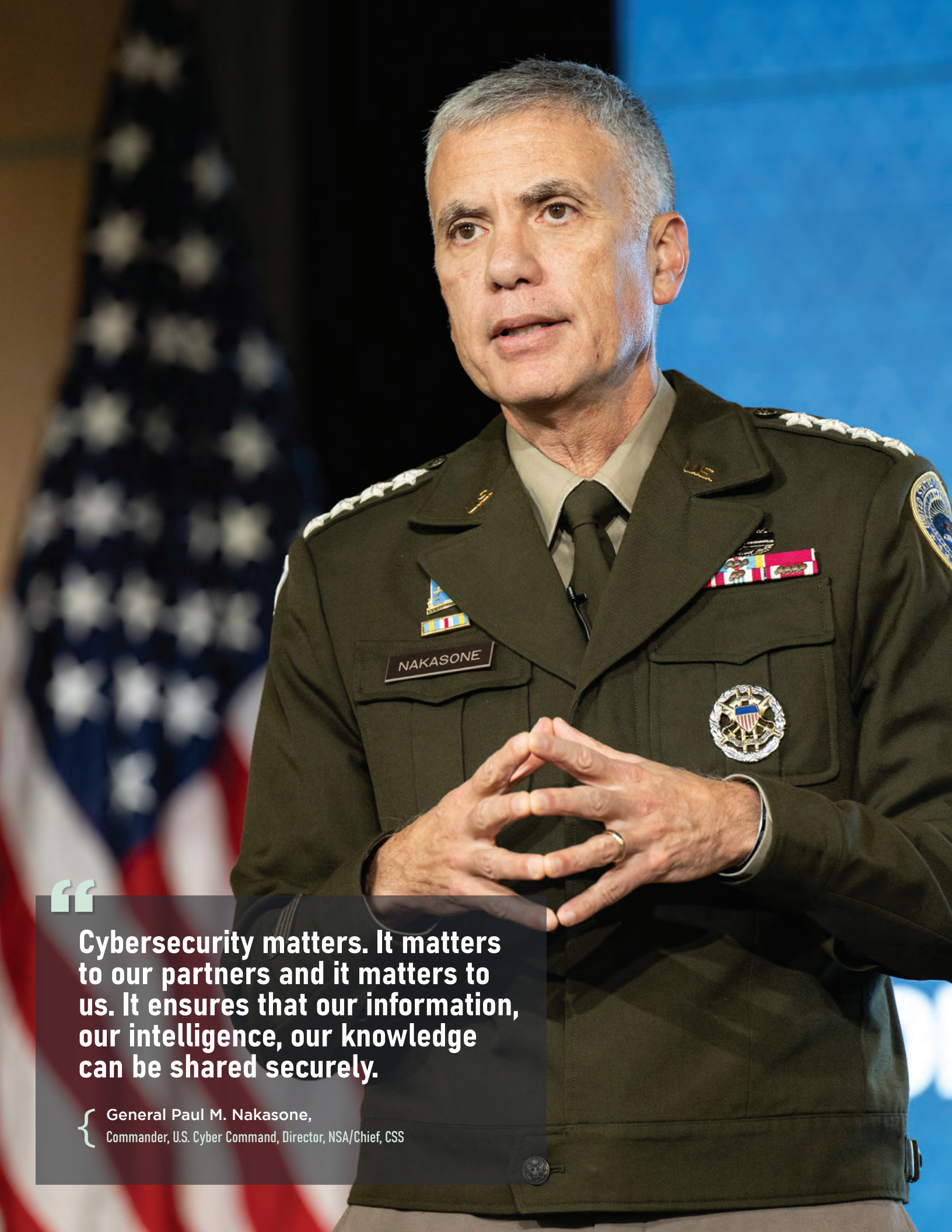
In 2023, the agency **completed cryptographic roadmaps for each U.S. combatant command** coalition partner. NSA used Command and Control Interoperability Board meetings between U.S. warfighting commands and their partners to identify critical missions employing obsolete cryptography and direct mission-driven modernization, an approach that baselines the partners' cryptographic posture, maps the crypto to specific weapon platforms, and maps the platforms to mission support. This effort pinpoints where resources must be committed to ensure partners are secure against advanced cyber threats across the warfighting domains and fully interoperable with U.S. and allied forces.

Through the DoD Strategic Cybersecurity Program, NSA worked in concert with DoD leaders and the U.S. military services to **assess their systems** and deliver plans to mitigate vulnerabilities, modernize cryptography, and monitor the systems. In the future, NSA plans to scale this activity through continued collaboration with the military services to perform additional cybersecurity assessments on priority systems. NSA also provided **operational support to military exercises** and planning conferences.

NSA continues to orchestrate and execute **cybersecurity risk evaluations** of DoD's most critical systems, helping DoD ensure that its systems continue to improve and harden in the face of persistent and tenacious cyber threats. Within the past year, NSA provided Zero Trust reviews and implementation roadmaps for two critical systems for the Navy and Air Force. The products were the result of enduring collaboration with the Navy and Air Force throughout the year.



Photos courtesy of Getty Images



Cybersecurity matters. It matters to our partners and it matters to us. It ensures that our information, our intelligence, our knowledge can be shared securely.

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



Aiding Interoperable Missions

NSA continues to represent the U.S. in NATO's information assurance and cyber defense capability panel, strengthening relationships with partner nations and focusing on driving platform and equipment modernization to aid **interoperable missions**. As the U.S. continues to modernize cryptography, NSA shares advanced cryptographic logic with capable NATO partners to help modernize the NATO enterprise and alliance. This year, NSA emphasized the work NIST performed developing quantum resistant capabilities. The panel is developing technical guidance and cybersecurity information sharing across NATO to secure critical networks from advanced cyber threats.

Furthering Nuclear Command, Control, and Communications (NC3) Cybersecurity

In 2023, NSA continued to partner with agencies across the DoD to prevent and eradicate cyber threats to Nuclear Command and Control Systems, focusing efforts to strengthen and cultivate partnerships. These relationships will be pivotal in scaling cybersecurity practices and leveraging innovative successes.

Fueled by a key partner, U.S. Strategic Command, NSA delivered a prototype capability to leverage sensing and monitoring, and provided visualization to deliver deep insight into the Nuclear Command, Control, and Communications (NC3) enterprise. NSA will continue to harness big data to inform decisions that will harden systems and eradicate threats.

NSA also established new and strengthened existing partnerships to deliver NC3 Strategic Cybersecurity Program evaluations providing cybersecurity risk, mitigation plans, and defensive monitoring recommendations for fielded systems. This year's operational support during war-game exercises provided DoD partners with real examples of how to prevent and eradicate threats to weapons and space systems.

Securing NSS with Commercial Solutions

NSA's Commercial Solutions for Classified (CSfC) program enables customers to **layer commercial solutions to protect classified information**. CSfC Capability Packages protect NSS by offering a robust systems approach for U.S. military services, combatant commands, and other federal partners.

CSfC allows customers to quickly configure and deploy secure cybersecurity solutions using NSA's preapproved systems-level designs and commercially available components to meet a wide range of mission use cases – not only within and between secure facilities, but also to enable remote access for telework and work that occurs outside of standard workspaces.

In 2023, CSfC continued to improve and update its publicly available Capability Packages, which guide customers toward implementing their own solutions. This year, CSfC published the supplemental guidance created for thin end user devices and private keys.

NSA also provides assurance of fielded solutions for customers such as the FBI and other critical systems. CSfC conducted an on-site assessment of four customers' CSfC registrations, which compares the registered solution with what was actually fielded by the implementing organization. NSA ensured that configurations, monitoring, and administration were in line with CSfC Capability Package requirements. This provides an opportunity for mutual technology enrichment and sharing, while capturing opportunities to improve the security and clarity of the requirements. NSA plans to continue these assessments in the future.





1000

010

0101 0110 010 1000

0101 0110 010 1000

0101 0110 010 1000

0101

10 010 1000

Researching

Cybersecurity Solutions

NSA's Laboratory for Advanced Cybersecurity Research remains at the forefront of protecting and securing our nation's cyber ecosystem, through robust and thriving partnerships with academic institutions, federally-funded research labs, and the private sector. NSA is uniquely positioned to bring world-class technical expertise to support whole-of-government efforts to ensure the United States' enduring advantage in Artificial Intelligence and Machine Learning. NSA's scientists, engineers, and thought-leaders have led and advanced research, tradecraft, and capabilities in data science for years, and our subject-matter expertise will be called upon to deliver secure development, integration, and adoption of AI capabilities within U.S. National Security Systems and the Defense Industrial Base.

Other recent cybersecurity research advances include:

- Strengthening cybersecurity standards in future technologies and forums critical to the nation, such as the 3rd Generation Partnership Project, which serves as the premier 5G standards entity.
- Provisioning foundational supply chain guidance to National Security System and Defense Industrial Base network defenders, ensuring the integrity of devices such as desktops, servers, and laptops involved in all enterprise-based procurement activities.
- Concluding the latest iteration of NSA's Science of Security Program, which promotes foundational cybersecurity research at academic institutions in cutting-edge science and emerging technologies, and kicking off the next version, sponsoring a series of new projects across seven different universities. The Science of Security program invites collaboration between academia, industry, and government to advance cybersecurity through scientific rigor.
- Developing cyber operator courses designed to equip the next generation of cyber professionals with cutting-edge skills to assess software vulnerabilities and protect our national cyber assets.



WOMEN immersed in **NSA** for cybersecurity

Developing

The Current and Next Generation of Cyber Experts

Enhancing the Cyber Workforce

Sponsored by the White House Office of the National Cyber Director, NSA partnered with other federal agencies to draft and publish the first-ever **National Cyber Workforce and Education Strategy**, approved by the Biden-Harris Administration in July. This strategy was designed with a people-focused component to augment National Cybersecurity Strategy that President Biden signed in March, and features four key pillars:

- Equip Every American with Foundational Cyber Skills
- Transform Cyber Education
- Expand and Enhance the Cyber Workforce
- Strengthen the Federal Cyber Workforce

The strategy was developed in consultation with industry, academia, non-profit organizations, and government partners. NSA contributed to the strategy and participated White House working groups, focusing on cyber education efforts and the federal cyber workforce. NSA's commitments include a pilot initiative to help develop "cyber clinics" across the nation which will support communities and small governments that would otherwise not have access to cyber risk assessment and planning assistance. The clinics will also provide an opportunity for more than 200 students to develop competencies while in a supervised learning environment.

Spotlighting and Recruiting Women in Cybersecurity

NSA's Cybersecurity Collaboration Center is leading the charge with academic, industry, and government partners to encourage more women to pursue careers in cybersecurity.

Following last year's successful Women Immersed in NSA Cybersecurity (WIN-Cyber) pilot, five new schools and twenty eager students participated in WIN-Cyber '23, hosted at the Cybersecurity Collaboration Center.

The WIN-Cyber program is a week long, immersive learning experience that allows students to collaborate and learn from some of NSA and U.S. Cyber Command's top cybersecurity professionals. WIN-Cyber '23 participants were nominated by their respective professors and represented schools including a 2-year community college, a Historically Black College and University, a Hispanic Serving Institution, and a 4-year public university. Students learned about NSA's cybersecurity mission and many have returned to their schools as NSA "ambassadors" who advocate for public service on their campuses.



Photo taken at the WIN-Cyber '23 event



Partnering with Academia

NSA continues to execute its cybersecurity academic strategy to inspire the cyber warriors of tomorrow through initiatives such as:

The **NSA Codebreaker Challenge** provides students attending U.S.-based academic institutions the chance to sharpen their cyber skills and gain experience in realistic NSA mission-centric scenarios. Through December 21, students are working to interpret and discover an unknown signals origin identified by the U.S. Coast Guard. Students are presented with a series of nine increasingly complex tasks to locate and analyze what produced the signal, discover an active collection operation tasked by a rogue server, and subvert the rogue server to stop the collection device.

The **GenCyber** program offers year-round cybersecurity training to students and teachers at the secondary level. This annual competitive program is offered to educational institutions and not-for-profit and non-profit institutions by way of an academic institution. Proposers can submit for four types of programs: student, teacher, combination and student language. In 2023, 160 programs were funded across 47 states, plus District of Columbia and Puerto Rico, serving approximately 5300 students and teachers. NSA and the National Science Foundation make this possible.

The **NSA Cyber Exercise (NCX)** develops future military and civilian cyber warriors and leaders by developing and testing their cybersecurity skills, teamwork, planning, communication, and decision-making. This annual exercise is the competitive cyber event of the year for the U.S. Service Academies, Senior Military Colleges, and NSA professional development program participants. The U.S. Air Force was awarded the 2023 NCX trophy.



Photo taken at the NCX 23' event.

The **NSA Experiential Tour** provides four-to-six week tours within NSA, U.S. Cyber Command, and partners to nearly 200 service academy, Senior Military College, and select Reserve Officer Training Corps (ROTC) members. These tours provide both classified and unclassified experiences, allowing participants to shape mission as they prepare to assume leadership roles.

Advancing the Study of Cybersecurity

NSA is invested in promoting cybersecurity careers throughout all levels of education. NSA's **National Cryptologic University runs the National Centers of Academic Excellence in Cybersecurity (NCAE-C)** program creates and manages a collaborative cybersecurity educational program with community colleges, colleges, and universities that:

- Establishes standards for cybersecurity curriculum and academic excellence
- Includes competency development among students and faculty
- Values community outreach and leadership in professional development
- Integrates cybersecurity practice within the institution and across academic disciplines
- Actively engages in solutions to challenges facing cybersecurity education

More than 400 schools have received the NCAE-C designation in designations of cyber, cyber defense, and cyber research.



Photo courtesy of Getty Images.

