NSA CYBERSECURITY YEAR IN REVIEW 2022

WELCOME

The National Security Agency (NSA) and its predecessors have been protecting the United States' most sensitive information since World War II. As communication technology and information technology have advanced — creating a more interconnected world with an increasing number of threats — NSA's mission has expanded and it has embraced new responsibilities and operational authorities to ensure our networks remain secure.

Today, NSA's cybersecurity mission integrates its cryptographic expertise, signals intelligence, vulnerability analysis, defensive operations, and more to prevent and eradicate cyber threats to:

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, operate, and maintain 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.

While much of the critical work 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. Visit NSA.gov/cybersecurity to access the report digitally. Provide NSA Cybersecurity with feedback or ask questions by emailing cybersecurity@nsa.gov.

TABLE OF CONTENTS

LETTER FROM THE NSA CYBERSECURITY DIRECTOR 02

RESPONDING TO NATIONAL THREATS AND PRIORITIES 04

PARTNERING WITH INDUSTRY 08

ARMING NET DEFENDERS WITH GUIDANCE 16

DEFENDING OUR MOST CRITICAL NETWORKS 19

CREATING CRYPTOGRAPHY TO PROTECT DATA, COMMUNICATIONS 22

PROTECTING THE WARFIGHTER AND SUPPORTING THE COMBATANT COMMANDS 26

RESEARCHING CYBERSECURITY SOLUTIONS 31

DEVELOPING THE CURRENT AND NEXT GENERATION OF CYBER EXPERTS 34

LETTER FROM THE NSA CYBERSECURITY DIRECTOR

CYBERSPACE IS DANGEROUS

More than a month before Russian troops invaded Ukraine in February, a cyberattack took down several of Ukraine's government websites.

An ominous message greeted visitors: "... be afraid and expect the worst. This is your past, present and future."

While Europe hasn't seen this level of kinetic activity since World War II, this hybrid war started in cyberspace. It's an environment where actors can increase their power, degrade others, and gain a strategic advantage — often at a very low cost.

In the weeks leading up to and following Russia's invasion in Ukraine, at least seven new families of destructive data wipers were used. One even attacked satellite broadband service to disrupt Ukraine's military communications on the day of the invasion but spilled beyond the conflict, impacting critical infrastructure remote monitoring of wind turbines in Germany, emergency services in France, and internet access of select users in Europe. Industry observed and reported on many of these destructive wipers, demonstrating their unique insights into the conflict.

The Russian threats did not stop with Ukraine. Hacktivists targeted our Defense Industrial Base and the communications and weapons systems of EUCOM and NATO were in the crosshairs of our adversaries. The keys, codes, and cryptography we provide are vital: Encryption is the last line of defense.

We are driving security outcomes by sanitizing and sharing our secrets.

Our focus extends beyond the Russia-Ukraine conflict, but this example demonstrates the complex environment. Our approaches must scale for China, Iran, North Korea, cybercrime, and other threats.

In addition to the insights we receive from industry, we are committed to contributing our unique value to the conversation: foreign intelligence, practical experience with exploitation tradecraft, and deep technical expertise of our adversaries.

Often, what we know is not as sensitive as how we know it. Our insights are useless unless someone can take action with them. We empower our industry partners to act on that information, and benefit from both their action and their insights.

Our Cybersecurity Collaboration Center (CCC) has formed hundreds of industry partnerships with the goal of better protecting our Defense Industrial Base and sensitive government systems. The intelligence picture we build, and security improvements we make together, scale far beyond defense contractors. For example, we reach a cumulative, estimated 2 billion endpoints through sharing info to technology providers and cybersecurity companies.

By protecting our most sensitive networks, we help protect yours.

We aren't just throwing our partners an IP address over our barbed-wire fences, either. In the last year, we've performed 10,000 robust bidirectional exchanges through our CCC. We work with industry to investigate the unknown and our partners often take actions that have global implications, such as issuing patches for zero-day vulnerabilities before our adversaries can perform widespread exploitation.

These efforts are critical because our adversaries are conducting increasingly sophisticated and broad intrusions with consequences that transcend international borders. For our most important secrets, they will go to significant lengths and we must defend with rigor and depth.

We must form collaborative campaigns to counter nation-state and cybercriminal threats that put our national security at risk. They have to combat immediate threats like Russia as well as pervasive threats like China.

Our aptly-named Adversary Defeat team is leading the charge in this area by collaborating with our interagency partners to generate outcomes against our highest priority threats.

We work across a wide array of departments and agencies, each with unique, complementary authorities, capabilities, and cultures.

When we each come to the table with a shared objective, we can disrupt and degrade malicious cyber activity.

As the scope of malicious cyber incidents and the sophistication of our adversaries grow, it will take a unified public-private sector strategy to gain the competitive advantage in this environment.

Our power is in partnerships. Strategic collaboration across security and intelligence spheres, and across classified and unclassified settings, results in increased speed and agility.

We are preparing for the transition to quantum-resistant cryptography to protect ourselves into the future. That protection not only goes into our networks, but the weapons platforms and other technology we rely on. We have to recognize networked computers are in every facet of our environment and change culture to secure all of them. Tools like National Security Memorandum 8 that give directive authorities to improve the cybersecurity of National Security Systems are improvements that enable such action.

Cybersecurity is national security and we all have an important role to play. We need leaders who recognize the threat, drive a culture that emphasizes robust security, and lean on partnerships. Leaders must emphasize a culture of cybersecurity and provide their teams with resources to secure their systems. We need cybersecurity at scale.

Regards,

Rob Joyce

Rob Joyce
Director, NSA Cybersecurity

RESPONDING TO NATIONAL THREATS AND PRIORITIES

COUNTERING GLOBAL THREATS

NSA and its U.S. and international partners scale impact against global threats by collaborating on coordinated responses.

While the U.S. Government relies on NSA's unique foreign signals intelligence insights to inform key decisions, each private and public sector partner builds on that foundation to create a more comprehensive understanding of the threat and what should be done to counter it.

Each partner also brings their own unique authorities and capabilities to the fight. This enhances our collective ability to prevent and eradicate some of the world's most concerning cyber threats.

NSA joined U.S. partners — the Cybersecurity and Infrastructure Security Agency (CISA), U.S. Cyber Command, and the Departments of Justice, State and Treasury — as well as international partners — the Australian Cyber Security Centre, the UK's National Cyber Security Centre, and Canada's Communications Security Establishment and Canadian Centre for Cyber Security — to publish a Cybersecurity Advisory to disrupt and degrade a multi-year global ransomware threat that affected hundreds of organizations.

Iranian Islamic Revolutionary Guard Corps (IRGC)-Affiliated Cyber Actors were exploiting publicly known vulnerabilities to gain access to networks around the globe. The malicious state-sponsored actors then encrypted

> The combined talent of our partners is the greatest competitive advantage we have to confront the increasingly sophisticated threats to our nation. Through partnerships, we bolster and enable defense, and disrupt and degrade adversary activities.
>
> **General Paul M. Nakasone,**
> **Commander, U.S. Cyber Command,**
> **Director, NSA/Chief, CSS**

PHOTO COURTESY OF JOSEPH BARILLARI

Iranian Islamic Revolutionary Guard Corps-affiliated actors were planning to ransom Boston Children's Hospital, according to the FBI.

information and extorted data to support ransom operations. The actors victimized a broad range of organizations, including small businesses, government agencies, nonprofit programs, and educational and religious institutions. Their victims also included multiple critical infrastructure sectors, including health care, transportation services, and utility providers.

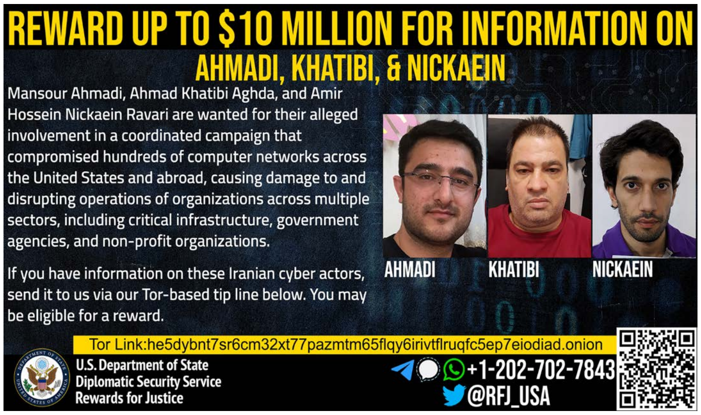
On September 14, the international coalition released, "Iranian Islamic Revolutionary Guard Corps-Affiliated Cyber Actors Exploiting Vulnerabilities for Data Extortion and Disc Encryption for Ransom Operations." The Cybersecurity Advisory alerted network defenders of the threat and armed them to defend against it. The advisory shared the actors' tactics, techniques, and procedures (TTPs) — mapped to the MITRE ATT&CK framework — and provided guidance on how to detect and mitigate against the threat. Because hundreds of companies, organizations, and institutions were compromised around the globe, the advisory was shared with U.S. and international victims directly and partners amplified the guidance upon release to prompt net defenders to act.

On the same day, U.S. partners held the actors and the Iranian government responsible for their malicious behavior and their failure to observe international cyber norms.

- The Department of Justice unsealed an indictment charging three Iranian nationals with engaging in ransomware-style extortion against U.S. critical infrastructure providers.
- The Department of Treasury's Office of Foreign Assets Control sanctioned 10 actors and two entities.
- The Department of State Rewards for Justice released a notification offering a reward of up to $10 million for information on three IRGC employees.

By increasing awareness and helping to secure systems, NSA and its partners degraded the malicious activity.

PHOTO COURTESY OF U.S. DEPARTMENT OF STATE



REWARD UP TO $10 MILLION FOR INFORMATION ON
AHMADI, KHATIBI, & NICKAEIN

Mansour Ahmadi, Ahmad Khatibi Aghda, and Amir Hossein Nickaein Ravari are wanted for their alleged involvement in a coordinated campaign that compromised hundreds of computer networks across the United States and abroad, causing damage to and disrupting operations of organizations across multiple sectors, including critical infrastructure, government agencies, and non-profit organizations.

AHMADI KHATIBI NICKAEIN

If you have information on these Iranian cyber actors, send it to us via our Tor-based tip line below. You may be eligible for a reward.

Tor Link:he5dybnt7sr6cm32xt77pazmtm65flqy6irivtflruqfc5ep7eiodiad.onion

U.S. Department of State
Diplomatic Security Service
Rewards for Justice

+1-202-702-7843
@RFJ_USA

The State Department offered a reward of up to $10 million for info on three IRGC-affiliated actors.

PHOTO COURTESY OF GETTY IMAGES

NSA and its partners released three Cybersecurity Advisories in early 2022 about potential Russian threats to U.S. critical infrastructure, including the energy sector.

DEFENDING THE HOMELAND AGAINST RUSSIA

As Russia invaded Ukraine in early 2022 and the U.S. held Russia accountable, intelligence indicated that the Russian government was exploring options for potential cyberattacks against the U.S., including its critical infrastructure sectors.

NSA, CISA, and FBI issued Cybersecurity Advisories in January, February, and April to heighten awareness of the threat and promote understanding of Russian state-sponsored and cybercriminal tactics, techniques, and procedures (TTPs) so that net defenders could strengthen their defenses.

Through operational collaboration with Defense Industrial Base companies and their service providers, NSA's Cybersecurity Collaboration Center (CCC) played a leading role in protecting key critical infrastructure sectors. The CCC conducted more than 2,000 bidirectional exchanges in the first four months of 2022, sharing NSA's insights, actionable information on Russian cyber TTPs, and building a more fulsome intelligence picture with industry's help.

Throughout the conflict in Ukraine, NSA has provided foreign signals intelligence insights that have aided U.S. Government leaders, NATO and the U.S. European Command

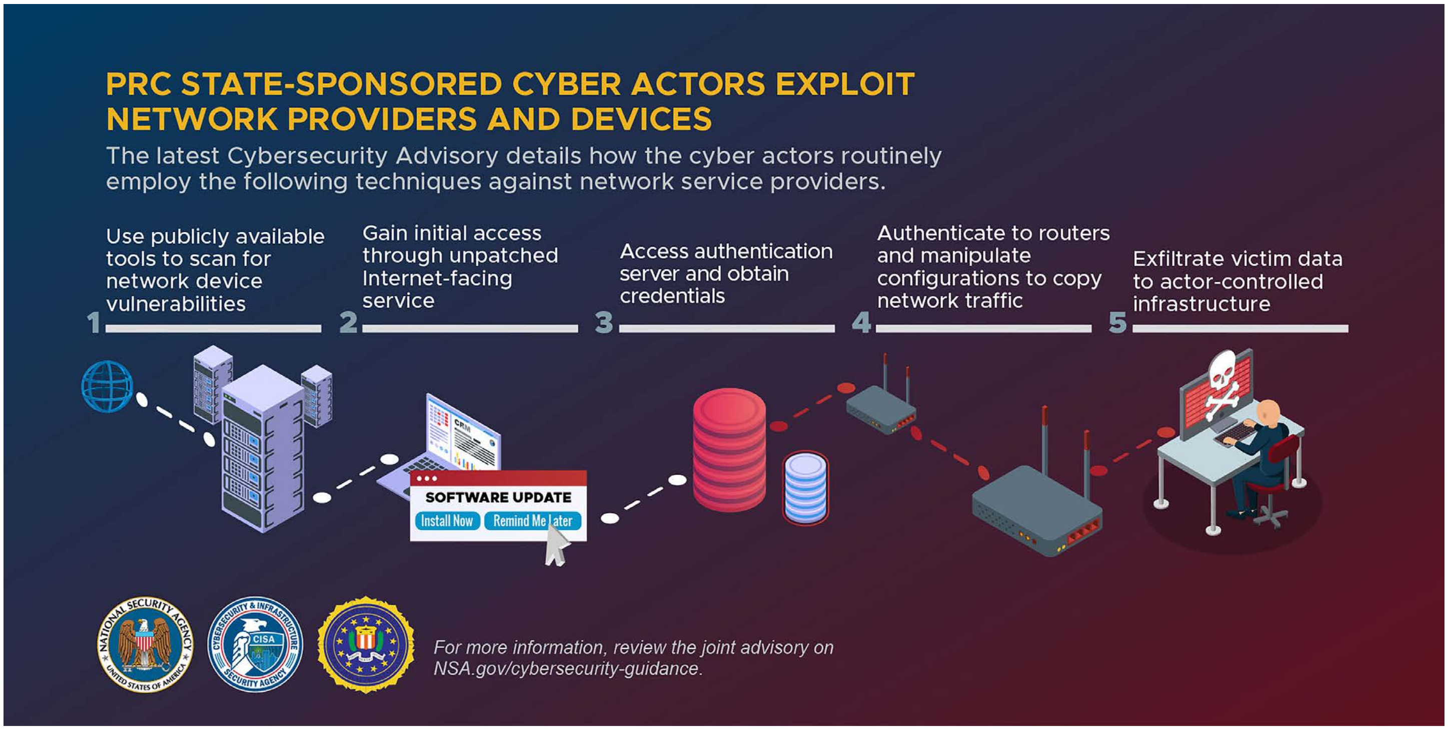
(EUCOM). It has also provided cryptographic security products to meet unplanned emergent requirements and to support urgent missions. It has rapidly deployed more than 150 communications security (COMSEC) devices to support mission operations during the global crisis.

EXPOSING CHINA'S MALICIOUS ACTIVITY

NSA continues to highlight the Common Vulnerabilities and Exposures (CVEs) and TTPs that People's Republic of China (PRC) state-sponsored cyber actors rely on to compromise systems and steal sensitive information. In June, NSA partnered with FBI and CISA to release the Cybersecurity Advisory, "People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices."

The advisory discusses how PRC actors have established a broad network of compromised infrastructure. They've compromised major telecommunications companies and network service providers primarily by exploiting publicly known vulnerabilities.

The details in this advisory make it clear that network devices, including small office/home office (SOHO) routers and network attached storage devices, can be a security risk and should be secured by patching and disabling unnecessary ports and protocols.



PRC STATE-SPONSORED CYBER ACTORS EXPLOIT NETWORK PROVIDERS AND DEVICES

The latest Cybersecurity Advisory details how the cyber actors routinely employ the following techniques against network service providers.

1 Use publicly available tools to scan for network device vulnerabilities

2 Gain initial access through unpatched Internet-facing service

3 Access authentication server and obtain credentials

4 Authenticate to routers and manipulate configurations to copy network traffic

5 Exfiltrate victim data to actor-controlled infrastructure

For more information, review the joint advisory on NSA.gov/cybersecurity-guidance.

NSA released a Cybersecurity Advisory that highlighted how People's Republic of China actors were exploiting network service providers and their devices.

AIRBORNE

PARTNERING WITH INDUSTRY

OPERATIONALIZING INTELLIGENCE THROUGH PRIVATE-SECTOR PARTNERS

NSA's Cybersecurity Collaboration Center (CCC) plays a key role in whole-of-government and international efforts to advance cybersecurity. NSA brings unique resources to the fight: Its foreign signals intelligence (SIGINT) system and cybersecurity operations across National Security Systems (NSS) generates unique insights into nation-state intentions and capabilities in cyber. At the CCC, NSA fuses those insights with those from private-sector partners to deliver intel-driven cybersecurity that protects the nation and U.S. allies.

The CCC defends the U.S. Defense Industrial Base (DIB) and disrupts the adversary by sharing timely threat intelligence with high-impact partners, best positioned to scale detection and mitigation techniques to billions of endpoints.

In 2022, the CCC nearly tripled its partnerships, growing from 110 partners to more than 300 collaborative relationships. The CCC's partners now reach a cumulative, estimated 2 billion endpoints, and its DIB prime partners account for 80 percent of Department of Defense (DoD) acquisition spending.

In the past year, the CCC also doubled its analytical exchanges with these partners. Thanks to more than 10,000 bidirectional collaborations — primarily focused on Russian and People's Republic of China (PRC) cyber threats and responding to world events — billions of endpoints have been hardened against nation-state threats.

For example, if NSA shares a nation-state actor's malware or tactics, techniques, and procedures (TTPs) with an internet service/cloud provider with a global footprint, the provider can develop and deploy signatures to defend against the threat at scale. While the CCC's primary goal is to defend the DIB, its efforts cascade protection across all 16 U.S. critical infrastructure sectors, reach businesses and consumers, and even protect our allies.

In late 2020, NSA opened the Cybersecurity Collaboration Center, an unclassified facility outside the NSA-Washington fence line. This year, the CCC expanded to four new satellite locations: Georgia, Texas, Hawaii, and the United Kingdom.

> Our partnership with industry goes beyond intelligence sharing. It's better defined as operational collaboration. By building trust, talking continuously, and focusing our efforts on shared priorities, we're achieving incredible outcomes.
>
> **Morgan Adamski,**
> **NSA Cybersecurity Collaboration Center Chief**

OUR INDUSTRY PARTNERS ARE SAYING:

> "NSA's PDNS and vulnerability scanning are incredibly valuable. They are helping us illuminate our supply chain and provide better protection to small companies who need it."

DISCLOSING ZERO-DAY VULNERABILITIES

To see how NSA's partnerships help secure the world, look no further than its work to discover and disclose vulnerabilities in core technology products. In 2022, the CCC disclosed dozens of zero-day vulnerabilities to vendors, ensuring dangerous bugs can be remediated.

For example, the CCC partnered with the United Kingdom's National Cyber Security Center (NCSC) this year to jointly disclose a critical cryptographic vulnerability in Microsoft Windows. The vulnerability could allow attackers to manipulate public certificates that spoof their identity and perform actions such as authentication or code signing.

In the hands of a capable adversary, the flaw could have very potent impacts. Thanks to the power of NSA's industry and international partnerships, the vulnerability was quickly disclosed to Microsoft and patched for all users running supported versions of Windows through automatic updates.

> In 2022, the CCC disclosed dozens of zero-day vulnerabilities to vendors, ensuring dangerous bugs can be remediated.

> While the CCC's primary goal is to defend the DIB, its efforts cascade protection across all 16 U.S. critical infrastructure sectors, reach businesses and consumers, and even protect our allies.

This was the first joint vulnerability disclosure between NSA and an international partner.

SCALING DIB DEFENSE

To protect sensitive U.S. Government information, combat the PRC's theft of intellectual property, and ensure small-to-medium-size businesses (SMBs) benefit from strong cyber hygiene, the CCC provides NSA-managed, no-cost cybersecurity services to more than 150 enrollees. This ensures SMBs don't have to defend against nation-state threats alone.

NSA's suite of cybersecurity services are infused with technical indicators of known malicious activity that are derived from its SIGINT mission. Its Protective Domain Name System (PDNS) service alone is clearing close to 100 million DNS queries daily, and has blocked around 400 million malicious

At the Cybersecurity Collaboration Center, industry and government experts can collaborate to counter malicious activity.

It is also critically important to measure success. The CCC tracks key performance indicators on a monthly and quarterly basis for quantitative feedback, but it also receives qualitative feedback.

"We get this feedback from both our industry partners, and, thanks to our global SIGINT system, we get feedback directly from our adversaries, too," said Morgan Adamski, CCC Chief. "So we know that this operational collaboration is making an impact."

domains to date. That includes nation-state spear-phishing attempts, malware and, botnets.

The CCC has also used its PDNS analytics, which are informed by NSA's big data analysis expertise, to enable more successes. NSA analytics have identified domains that are not known to be malicious, but the behavior of the DNS call-out is consistent with malware. NSA then shared those insights with its PDNS provider, who identified and eradicated nation-state malware on DIB networks.

The CCC also offers threat intelligence collaboration services. These are underpinned by voluntary sharing agreements and mutual non-disclosure provisions that allow DIB companies to share company-sensitive information with the CCC. In turn, the CCC can share sensitive threat information relevant to the participating companies. This enables sharing tippers and threat reporting, enriching public-private understanding of shared threats, and creates the ability to benefit from each other's insights and data pools.

Through its vulnerability scanning and remediation services, the CCC also works with willing DIB partners to identify and resolve vulnerabilities prior to their exploitation. This enables the CCC to proactively engage with partners on issues before they become compromises. The CCC provides tailored reports that help companies prioritize their vulnerability management based on:

- Where they might have assets they didn't know about
- Where they might be vulnerable
- How they should then prioritize those vulnerabilities based off of severity and current nation-state targeting

NSA consistently receives feedback that this context of "what should I prioritize and when" is really helpful to DIB SMBs.

To date, the CCC has focused on enrolling companies that support critical DoD programs for cryptography, weapons and space, and nuclear command and control, but in 2023, the CCC is focused on scaling these services to thousands of qualifying companies. These services are available to any company that has an active DoD contract (sub or prime) and has access to non-public DoD information. To enroll, visit cybercenter.NSA.gov or email DIB_Defense@cyber.nsa.gov.

DEVELOPING CONSENSUS-BASED, INDUSTRY-DRIVEN STANDARDS

Standards have traditionally been viewed as an economic tool. Recent changes in standards development processes make it clear that they are also a national security tool. Standards are critically important because they:

- Directly underpin national security and the economy by integrating security into products early in their development
- Reduce the risk that manufacturers and their customers become victims of exploitation because of insecure or weak technologies
- Allow for interoperability between technologies, so the U.S. is not reliant on single market vendors

NSA's Center for Cybersecurity Standards (CCSS) is directly securing standards for

> These services are available to any company that has an active DoD contract (sub or prime) and has access to non-public DoD information.

OUR INDUSTRY PARTNERS ARE SAYING:

"I applaud NSA's PDNS efforts; initiatives to scale protections to the small businesses in our supply chain are critical and we want more."

emerging technology. NSA plays an important role in international standards development organizations (SDOs) because it possesses the technical expertise to draft strong standards and a vested interest in securing the technologies that impact national security and defense (e.g. cloud, 5G).

CCSS is focused on authoring, informing, and driving adoption of standards for telecommunications, with a focus on securing the 5G core, edge, and data in transit, cloud, and secure internet protocols, especially preparing protocols for quantum-resistant cryptography.

To date, CCSS has authored and submitted more than 35 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.

Through the Enduring Security Framework and CCSS, NSA has joined forces with industry

OUR INDUSTRY PARTNERS ARE SAYING:

"Our threat analysis group is focused on stopping APTs from using our platform. Our partnership with NSA is paving the way. They recently helped us stop a nation-state APT from abusing our platform to target the DIB."

J830-2 Stand 1-L
35 RESTRICTED AREA AUTHORIZED PERSONNEL ONLY
For Area Access or Assistance Please Contact Area Supervisor
40 PSF MAX
INNOVENTOR

PHOTO COURTESY OF DEFENSE CONTRACT MANAGEMENT AGENCY

Defense Industrial Base companies design, develop, operate, and maintain the Department of Defense's critical systems, platforms, and technologies required to defend the nation. Experts from NSA's Cybersecurity Collaboration Center work directly with these companies to protect sensitive information.

OUR INDUSTRY PARTNERS ARE SAYING:

> "Information sharing is good, but only if it is actionable. The CCC gives us actionable information."

NSA's Center for Cybersecurity Standards has submitted more than 35 standards for 5G, cloud, and internet protocols this year.

PHOTO COURTESY OF GETTY IMAGES

to reinvigorate U.S. and allied investment in Standards Development Organizations (SDOs). This ensures the long-term security of critical technologies. The group will assess technical and geopolitical threats to international SDOs and develop strategies to counter these threats.

NSA and its U.S. Government, industry and international partners increase awareness about the threats to standards and strategize to combat these threats. The greatest way to combat foreign adversarial influence in international SDOs is for like-minded nations — those that share the same values of security, privacy, and global market competition — to contribute technically sound standards proposals.

Commercial products are increasingly relied on to secure National Security Systems. Through the National Information Assurance Program (NIAP), the CCC certified 74 commercial components for protecting NSS. Additionally, NIAP published nine 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 continued to strengthen the global IT security posture through ongoing partnerships with 30 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 volunteered to take a leadership position in the CCRA by chairing the CCRA Management Committee through the end of 2023, to include leading integration with the European Union (EU) Cybersecurity Act.

NSA DIB CYBERSECURITY SERVICE OFFERINGS

DRIVE DOWN RISK | PROTECT DOD INFORMATION

To better protect sensitive information on Defense Industrial Base (DIB) networks, NSA offers the following **no-cost** cybersecurity services to companies with active DoD contracts and access to controlled information.

GOVSHIELD PROTECTIVE DNS

- Scalable GovShield PDNS service from Akamai.
- Real-time DNS malicious query interdiction.
- Integrates Akamai's commercial threat intelligence with NSA analytics and indicators of compromise.

VULNERABILITY SCANNING

- Leverages commercial and open-source information to expose vulnerabilities.
- Automated aggregation and reporting to companies.
- Identifies probable exploitation routes and engages before compromise.

THREAT INTELLIGENCE COLLABORATION

- Tailored distribution of NSA cybersecurity products.
- Timely and prioritized sharing of indicators of compromise and mitigations.
- Collaboration with NSA analysts on findings.

For more information on how to enroll in these services, email dib_defense@cyber.nsa.gov

cybercenter.nsa.gov

@NSACyber

PHOTO COURTESY: GETTY IMAGES

By clearly articulating the threats, NSA's reports help net defenders prioritize actions that degrade the malicious actors' capabilities and secure critical systems.

ARMING NET DEFENDERS WITH GUIDANCE

COLLABORATIVE REPORTS BUILD FULLER PICTURE

NSA's public reports are adorned with more agency seals than ever before, which speaks to the increased collaboration between U.S. and international partners around critical cybersecurity issues.

Whether it is mitigating against a significant vulnerability or defending against specific adversary and cybercriminal threats, U.S. and international agencies are capitalizing on opportunities to build a more comprehensive threat understanding and present top defensive actions with a coordinated voice. NSA collaborated with international partners on nearly two-thirds of its public cybersecurity releases from the past year.

Throughout 2022, NSA focused on producing guidance that is unique, timely, and actionable. It released its first of three Cybersecurity Advisories about Russian threats to U.S. critical infrastructure more than a month before Russia invaded Ukraine. NSA also highlighted new tactics, techniques, and procedures (TTPs) from People's Republic of China and Iranian state-sponsored actors.

These Cybersecurity Advisories attribute activity to specific nation-state and cybercriminal groups. By clearly articulating the threats, the reports helped net defenders prioritize actions that degrade the malicious actors' capabilities and secure critical systems. This makes it more difficult and more costly for these actors to compromise U.S. and allied networks. NSA also highlighted broader threats, such as ransomware trends, top exploited vulnerabilities, and how malicious actors take advantage of weak security controls.

NSA's technical experts aren't afraid to get in the weeds. They published lengthy technical reports on securing PowerShell scripting, network infrastructure guidance, protecting satellite communications, and even microelectronics hardware assurance best practices.

> The number of new reported vulnerabilities increases each year, making it hard for net defenders to prioritize patching and remediation efforts. Our publications help cut through the noise. We alert defenders to the highest priority cyber threats and provide actionable recommendations for mitigation.
>
> Neal Ziring, NSA Cybersecurity Technical Director

NSA CYBERSECURITY REPORTS

UNIQUE. TIMELY. ACTIONABLE.

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

NSA collaborates with U.S. and allied government partners as well as industry to share a comprehensive understanding of the malicious activity coming from nation-state cyber actors and cybercriminals.

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

NATIONAL SECURITY AGENCY · UNITED STATES OF AMERICA · CYBERSECURITY

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

Receive the latest alerts by following @NSACyber on Twitter.

DEFENDING OUR MOST CRITICAL NETWORKS

PRESIDENTIAL MEMO EXPANDS NSA'S AUTHORITY TO PROTECT KEY SYSTEMS

In January, President Joe Biden signed the "Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems." Better known as National Security Memo-8 (NSM-8), the memo set cybersecurity requirements for protecting some of the nation's most sensitive networks — National Security Systems (NSS) — that meet or exceed the requirements previously set in Executive Order (E.O.) 14028, "Improving the Nation's Cybersecurity."

NSM-8 provided the NSA Director, as the National Manager for NSS, with 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 U.S. Government. It also positioned NSA to set priorities — such as requiring that NSS owners mitigate against a vulnerability being exploited by our adversaries — and direction — such as requiring that owners employ proven cybersecurity solutions like multifactor authentication.

This increased responsibility led NSA to form even closer relationships with the more than 50 departments and agencies across the U.S. Government that own or operate NSS.

NSA established foundational policies, procedures, and workflows to improve the cybersecurity posture of critical U.S. Government systems, created inventories and databases to capture data, and supported U.S. Government efforts to update the Federal Acquisition Regulation, Defense Federal Acquisition Regulation Supplement, and other cyber-related directives.

Since the memo was signed, NSA has released nearly two dozen directives and memoranda leveraging the new authorities to improve the cybersecurity of NSS on topics such as:

- The process for identifying and inventorying critical NSS and non-compliant cryptography
- The requirements for implementing multifactor authentication and data encryption
- Mitigations for identified threats to or vulnerabilities within cross-domain solutions, VMware, and Atlassian Confluence

> National Security Memo-8 is a game-changer because it expanded NSA's authorities to protect National Security Systems. This gives us better cybersecurity oversight, allows us to mitigate more vulnerabilities, and requires that proven cybersecurity solutions be implemented.
>
> Rob Joyce, NSA Cybersecurity Director

Through partnerships with other federal agencies, increased visibility within the national security community, and increased authorities to mandate vulnerability remediation, NSA is drastically increasing the security of critical U.S. Government systems — protecting sensitive military and intelligence data from our adversaries.

RAISING THE BAR ON CROSS- DOMAIN SOLUTIONS

Cross-domain solutions allow information to be shared across international, government, agency, and classification boundaries through controlled interfaces. The U.S. Government relies on NSA's National Cross-Domain Strategy & Management Office for cross-domain solution capabilities and mission needs.

NSA set the "Raise the Bar" strategy for cross-domain solutions that protect classified information. It focuses on improving cross-domain solution security and capabilities for NSS in the stages of design, development, assessment, and implementation.

NSA significantly accelerated Raise the Bar compliance in 2022, while working closely with the vendor community on the development of remote management (RMAN) and remote monitoring (RMON) capabilities. Several of these products have entered the lab-based security assessment process for projected availability to the community in 2023. This increased capability will continue to improve the security posture of the greater NSS through better management and monitoring.

ADVOCATING FOR ZERO TRUST, CLOUD

Traditional cybersecurity centered on a perimeter-defense model is ineffective against malicious cyber actors. Once inside the network, the actors can move laterally, escalate privileges, and compromise the mission. The only way to protect critical resources is through a data-centric model.

Zero trust is a cybersecurity strategy and framework that embeds security throughout the architecture for the purpose of preventing, detecting, and responding to data breaches. This security model eliminates the idea of trusted or untrusted networks, devices, personas, or processes and instead constantly interrogates the trust relationships formed by entities on the network and denies access by default, only allowing access by an approved user and device.

To demonstrate the efficacy of zero trust architectures in a government environment, and to enable NSA to publish well-informed guidance to the community, NSA built the Native Zero Trust Cloud (NZTC) environment — a private cloud that implements zero trust principles at the advanced level of the Department of Defense (DoD) Maturity Model.

NSA's zero trust experts also partnered with the DoD CIO, Defense Information Systems Agency (DISA), Cybersecurity and Infrastructure Security Agency (CISA), and subject matter experts from across the U.S. Government and industry to provide guidance to national-level strategies and roadmaps, and publish reference architectures for successful implementation. These documents will be used by DoD commands, military services, agencies, and mission owners as guides

NSA is drastically increasing the security of critical U.S. Government systems — protecting sensitive military and intelligence data from our adversaries.

PHOTO COURTESY OF LANCE CPL. GAVIN UMBOH, U.S. MARINE

to help them modernize and harden their mission infrastructures.

The U.S. Government is increasingly moving to cloud computing environments. Because adversaries often target the cloud, NSA has a strategy to protect NSS, the Defense Industrial Base, and other critical infrastructure sectors in cloud, hybrid cloud, and multi-cloud environments. The agency is collaborating with industry, academia, and U.S. and allied government partners to improve the hardening of clouds, detection of threats, and the development of actionable, scalable mitigations.

RED, BLUE, HUNT TEAMS ASSESS CYBERSECURITY

NSA cybersecurity assessment teams conduct operations with U.S. Government and Defense Industrial Base partners to identify critical cyber vulnerabilities on their networks and provide mitigation strategies. This helps protect the underlying information technology across multiple domains from cyber adversaries.

NSA's red, blue, and hunt teams completed 27 assessments this past year against critical networks and platforms across the U.S. Government. They identified vulnerabilities on partner networks and significantly improved the security posture of our critical networks around the globe and our strategic weapons and space platforms.

In 2022, NSA evolved its model to conduct integrated red, blue, and hunt assessments. After a cleared defense contractor was compromised, NSA tested the updated model and discovered new adversary tactics, which empowered the contractor to prevent and eradicate these new threats. NSA shared the new threat intelligence with its industry partners.

NSA delivered 140,000 tamper-indicating products globally in 2022. These technologies prevent or detect physical exploitation of cryptographic equipment and classified material during shipping or deployment around the world.

140,000

PHOTO COURTESY OF U.S. ARMY STAFF SARGENT. CHRISTOPHER STEWART

CREATING CRYPTOGRAPHY TO PROTECT DATA, COMMUNICATIONS

PROTECTING OUR NATION'S MOST CRITICAL SECRETS

Through its keys, codes, and cryptography mission, NSA secures millions of devices around the world and manages the infrastructure to key those devices. That 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.

On the battlefield, this helps warfighters have confidence in their operational picture, differentiate between friend and foe, and securely conduct command and control.

“If you don't want the adversary to know about it, control it, or deny your use of it, then encryption is your last line of defense,” said Troy Lange, Chief, NSA Encryption Production and Solutions.

“Our goal is to implement quantum-resistant cryptography for all National Security Systems by 2033. That may sound like it's a long way off, but modernization at scale takes time. We have to plan now.”

Troy Lange, Chief,
NSA Encryption Production and Solutions

NSA works with its government partners to ensure key management functions, networks, systems, and communications devices used by the Department of Defense (DoD) are secure. It also delivers communications security best practices that ensure secure handling of cryptographic material used with these systems and devices.

In 2022, NSA supported 61 unique customers on critical operations such as GPS key for U.S. Space Command. NSA also provided support to combatant commands and government agencies, such as U.S. Strategic Command, U.S. Central Command, the Defense Information Systems Agency, the Department of Energy, the White House Communications Agency, and many more.

MOVING TO QUANTUM-RESISTANT CRYPTOGRAPHY

A cryptanalytically relevant quantum computer (CRQC) — once achieved — has the potential to break cryptographic systems that secure the internet and information systems worldwide today. The best defense against this looming technological threat is quantum-resistant cryptography.

President Joe Biden signed “Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems” — also known as National Security Memo 10

(NSM-10) — in May to direct U.S. Government agencies to migrate vulnerable cryptographic systems to quantum-resistant cryptography as part of a multi-year transition.

As the National Manager for National Security Systems (NSS), the NSA Director is responsible for overseeing this transition to quantum-resistant crypto across the 50-plus government departments and agencies that use NSS.

Because the quantum computing threat is a shared cybersecurity challenge for government and private partners, and even the public, forming strategic and tactical partnerships has been key.

NSA collaborated with the National Institute of Standards and Technology (NIST) — the U.S. government lead for commercial algorithm approval — as well as the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence Science and Technology (ODNI S&T) office, the DoD, and external standards organizations to take on the quantum computing threat.

PHOTO COURTESY OF GETTY IMAGES

Cryptography helps secure critical U.S. military communications.

NIST announced its quantum-resistant algorithm selections for standardization in July, paving the way for NSA to provide its recommendations for securing NSS. NSA cryptographers partnered closely with NIST throughout its selection process, analyzing the candidates against NSS cybersecurity requirements.

In September, NSA released its Commercial National Security Algorithm Suite 2.0 (CNSA Suite 2.0) through a Cybersecurity Advisory, fulfilling a key responsibility under NSM-10. The publication notified NSS owners, operators, and vendors of the future requirements for quantum-resistant algorithms for use in all NSS.

NSA is urging industry to plan now to adopt its quantum-resistant algorithm suite for NSS and NIST's cryptographic standards into their systems. Modernization at this scale takes time and the entire community must start resourcing now for an orderly transition.

Industry should plan for sufficient storage, bandwidth, and power in their products to allow a drop-in of the algorithms and parameters once they are standardized.

MORE ABOUT CNSA 2.0

The Cybersecurity Advisory specifies the conventions for using the NSA's CNSA Suite algorithms in Internet Protocol Security (IPsec). Developers and operators should visit NSA.gov/cybersecurity to learn more.

NSA certified the Secure Cyber Module (SCM), which provides cryptographic capabilities to the Explosive Ordnance Disposal (EOD) robots in advanced EOD and man-transportable robotic systems. The crypto embedded within the SCM provides confidentiality services to allow secure remote operation of EOD robots.

PHOTO COURTESY OF SGT. ANTHONY ORTIZ, 2ND MARINE LOGISTICS GROUP

Once industry submits their quantum-resistant technologies through NSA and National Information Assurance Partnership (NIAP) validation programs, their products will become available and the U.S. Government will then start the acquisition process to get products into national security networks.

MODERNIZING CRYPTOGRAPHY

The transition to quantum-resistant cryptography is just one example of how NSA is staying one step ahead of our nation's adversaries to protect our most sensitive data. NSA is continually modernizing its cybersecurity solutions to be agile, threat adaptive, and scalable across multi-domain operations. A few 2022 modernization successes include:

- NSA delivered another set of updated cryptographic devices that implement NSA-approved government off-the-shelf quantum-resistant algorithms to protect NSS from potential adversarial quantum computing attacks. The initial set was delivered in 2021. While a CRQC remains theoretical, the development and use of one could make key portions of the U.S. cryptographic inventory obsolete.
- NSA certified 21 high assurance cryptographic solutions in 2022, after ensuring that security requirements, tailored for each solution, were met. Many of these products are upgrades to strengthen the security of existing devices such as multichannel radios, tactical receivers, data links, and the GPS IIIF satellites. The certified products secure intelligence sharing, info for combat threat awareness, tactical data and voice, as well as space and weapons systems.
- NSA collaborated with partners to complete an initial assessment of 2022 NIST quantum-resistant cryptography selections in support of tactical use cases. The preliminary results indicate the selections will, in general, meet or exceed performance thresholds for use on tactical devices. These results improve NSA's advisement to tactical customers, program offices, and vendors on cryptographic implementation efforts. Faster implementation will accelerate adoption of quantum-resistant cryptography and mitigate quantum cryptanalytic threats.

PROTECTING THE WARFIGHTER AND SUPPORTING THE COMBATANT COMMANDS

SECURING TECHNOLOGIES AND PROMOTING INTEROPERABILITY

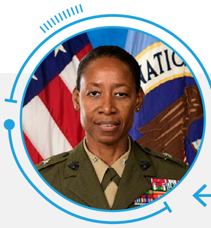
As a combat support agency under the Department of Defense (DoD), NSA supports U.S. military service members through its primary missions: foreign signals intelligence and cybersecurity.

NSA's foreign signals intelligence experts provide intelligence support to military operations, while its cybersecurity experts provide products and services that ensure military communications and data remain secure. NSA's keys, codes, and cryptography work secures everything from tactical radios on the warfighter to their critical weapons systems. This protects warfighters from U.S. adversaries and gives them an advantage on the battlefield.

Interoperability is crucial for the U.S. military when conducting joint operations and exercises. NSA and standards organizations set common protocols and standards so that the U.S. military can securely share information with U.S. allies, NATO, and coalition forces around the world.

NSA represents 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 modernizing cryptography, NSA is sharing advanced cryptographic logic with capable NATO partners to help modernize the NATO enterprise and alliance. Likewise, the panel is developing technical guidance and cybersecurity information sharing across NATO to secure critical networks from advanced cyber threats.

NSA is developing a key management strategy for secure distribution from cryptographic key generation to consumption by an end cryptographic unit or system that will include a modern approach of over-the-network keying.



> As our warfighters engage against sophisticated adversaries in competition and conflict, confidence in the security of their command and control, and weapon systems is an operational imperative. Delivering products and services to deny and deter the adversary while assuring security and creating advantage for the Joint Force capabilities is our raison d'etre.
>
> **Brigadier General Lorna Mahlock,**
> **NSA Cybersecurity Deputy Director for Combat Support**

NSA's cybersecurity experts provide products and services that ensure military communications and data remain secure.

PHOTO COURTESY OF GETTY IMAGES

Soldiers in the field rely on NSA for secure communications.

PHOTO COURTESY OF CPL. MOISES RODRIGUEZ, U.S. MARINE CORPS

NSA also took initial steps to transition NATO's legacy electronic key delivery system to a modern and secure key management infrastructure. For non-NATO nations, NSA installed a software-based black key delivery solution in four combatant commands, replacing an unsupportable, legacy system.

The agency is also building a cryptographic roadmap for each U.S. combatant command coalition partner. NSA attended 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, a three-phased 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.

EVALUATING WEAPONS AND SPACE CYBERSECURITY

NSA continued performing critical cybersecurity evaluations on some of the nation's most important weapons and space systems across all warfighting domains to ensure they aren't vulnerable to cyber adversaries.

Through its Department of Defense (DoD) Strategic Cybersecurity Program (SCP) Program Management Office, NSA worked in concert with DoD leaders and the U.S. military services to evaluate the systems and issue plans for mitigating vulnerabilities, modernizing cryptography, and recommendations for monitoring.

NSA also 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 (JFHQ-DODIN), NSA is reducing the chance that U.S. adversaries can access warfighter communications and sensitive data.

NSA works closely with U.S. Strategic Command to secure U.S. nuclear command and control systems.

PHOTO COURTESY OF UNITED STATES STRATEGIC COMMAND

NEXT-GENERATION NUCLEAR COMMAND, CONTROL AND COMMUNICATIONS (NC3) CYBERSECURITY

NSA helps secure communication between senior leaders and ensure command and control of strategic forces by preventing and eradicating cyber threats to U.S. nuclear command and control systems (NCCS) and the National Leadership Command Capability (NLCC).

Last year, NSA created a nuclear command, control, and communications (NC3) cybersecurity strategy and framework for the U.S. Strategic Command (USSTRATCOM) NC3 Enterprise Center (NEC). USSTRATCOM deters strategic attack and employs forces, as directed, to guarantee the security of the U.S. and its allies.

In 2022, NSA created a framework for securing the next-generation of NC3 networks. It focuses on three core areas — protection of data, protection of transport, and protection of interfaces — that will help secure and guide the development of the nation's most critical networks.

NSA also completed an effort to provide NC3 cybersecurity data ontologies to the NEC. As part of a larger NC3 Enterprise data ontology effort, these cybersecurity ontologies will enable effective and efficient information sharing, consistent responses to cyber events in the Next Generation NC3 enterprise, and enable interoperability of solutions developed by different vendors.

SECURING NSS WITH COMMERCIAL SOLUTIONS

NSA's Commercial Solutions for Classified (CSfC) program enables commercial technologies and products to be composed in layered solutions to protect classified information.

CSfC Capability Packages protect National Security Systems (NSS) by offering a

The annual CSfC Conference brings together industry vendors, trusted integrators and government organizations to discuss changes to Capability Packages, solution registration, CSfC component listing, the CSfC Trusted Integrator program, and more.

PHOTO COURTESY OF GETTY IMAGES

Visit NSA.gov/cybersecurity to learn how you can register a CSfC solution.

robust systems approach for U.S. military services, combatant commands, the Defense Information Systems Agency (DISA), FBI, and other customers. It allows them 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. This includes both within and between secure facilities, as well as remote access to support telework and mission outside of normal workspaces.

In 2022, CSfC continued to improve and update its publicly available Capability Packages, which guide customers toward implementing their own solutions. The Wireless Local Area Network (WLAN) Capability Package, for example, provides customers with enhanced security guidance and protections for operating campus wireless solutions.

Three new revisions to CSfC Annexes were published, improving the requirements for key management, symmetric key management, and the enterprise infrastructure for CSfC solutions. These updated Annexes will provide quantum-resistant encryption, and more efficient infrastructure for all CSfC solutions.

NSA also provides additional assurance of fielded solutions. For example, the CSfC program conducted an on-site assessment of a customer's CSfC registration, 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 do more of these assessments in 2023.

RESEARCHING CYBERSECURITY SOLUTIONS

SECURING AMERICA'S INFORMATION SYSTEMS OF TOMORROW

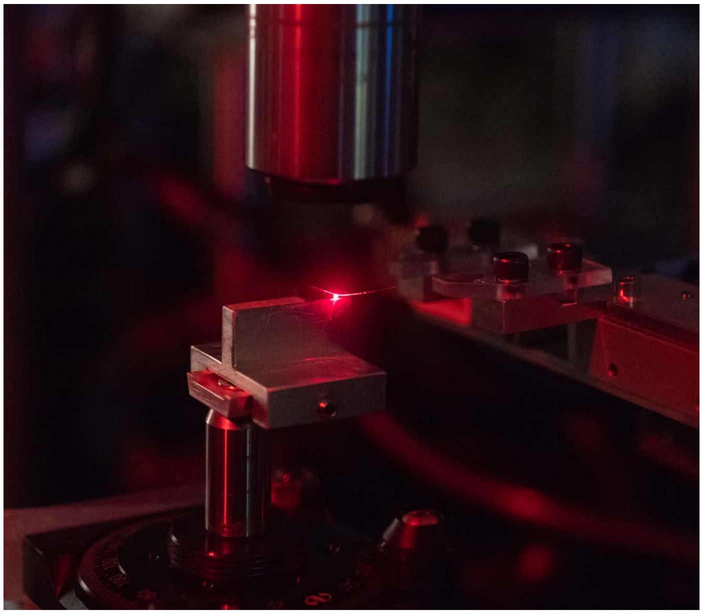
As the U.S. Government's premier cybersecurity research and development center, NSA's Laboratory for Advanced Cybersecurity Research delivers tools and technology advancements that protect and secure the nation's cyber ecosystem, from National Security Systems to everyday devices. For example, NSA researchers developed Security-Enhanced Linux (SELinux), which became the foundation for the Security-Enhanced Android operating system used by billions of smartphones worldwide.

NSA researchers achieve these outcomes by staying at the forefront of emerging

> To stay one step ahead of our adversaries, we must continue to learn about emerging technologies and deliver findings and new tools that protect our sensitive data and give our nation an advantage.
>
> **Gilbert Herrera, NSA Research Director**

NSA Research was behind Security-Enhanced Android, which is now used in billions of smartphones.

PHOTO COURTESY OF GETTY IMAGES



NSA researchers are exploring ways to incorporate tapered glass optical fibers into new technologies to maintain effectiveness at extreme temperatures. This scalable solution allows compatibility in retrieving data from superconducting computers.

technologies — such as artificial intelligence and machine learning — and adapting principles to the cybersecurity domain through partnerships with universities, federally funded research labs, and the private sector. These collaborations are revolutionizing NSA's collective ability to triage voluminous amounts of data into actionable and priority events of concern.

Other recent cybersecurity research advances include:

- Enhanced security of next-generation technologies poised to transform our warfighting capabilities, such as 5G, through the adoption of standards and industry best practices.
- Advanced software-analysis tools and guidance to ensure the cybersecurity community can defend software and hardware development from sophisticated cyberattacks.
- Hosted premier forums bringing together the best in government and industry to address top cybersecurity mission challenges, such as the 2022 International Conference on Machine Learning (ICML).
- Sponsored NSA's Science of Security (SoS) Program to encourage foundational cybersecurity research at academic institutions, promote rigorous research competitions, and inspire students to seek out careers supporting the nation's cybersecurity workforce. NSA served as a Special Award Sponsor at the 2022 Regeneron International Science and Engineering Fair (ISEF) in Atlanta, reviewing over 1,800 project submissions for awards in the categories of Cybersecurity, Principles of Security and Privacy, Mathematics, and Material Science.

USING MATH TO FIND THE ANSWERS

NSA performs mathematics research, analysis, and design of cryptographic algorithms that underpin the cybersecurity of high-assurance cryptographic solutions that protect nuclear command and control systems, space and weapons systems, U.S. Intelligence Community (IC) networks, Department of Defense networks, and NSA's Key Management Infrastructure.

In 2022, NSA's math researchers designed a new authenticated encryption algorithm for use in NSA's forthcoming high-speed encryption products. The team's solution is simple enough to run at incredibly high speeds without causing the encryptors to overheat, while simultaneously limiting their use of power. In addition, it provides protection against attacks that could result from the high volume of encrypted data.

Logic components for more energy-efficient operations in high-performance computing.

DEVELOPING THE CURRENT AND NEXT GENERATION OF CYBER EXPERTS

SPOTLIGHTING AND RECRUITING WOMEN IN CYBERSECURITY

Women comprise about 25 percent of the global cybersecurity workforce, according to a 2022 study by Cybersecurity Ventures. NSA is working with academic, industry, and government partners to encourage more women to pursue careers in cybersecurity.

NSA's Cybersecurity Collaboration Center (CCC) — where the workforce is more than 50 percent women — is leading the charge. For the past two years, the CCC has sponsored and participated in the Women in Cybersecurity (WiCyS) Conference. Participants have showcased NSA's cybersecurity mission and how diversity has helped NSA solve difficult problems.

The CCC also is helping to recruit the next generation of cyber experts. In August, General Paul M. Nakasone, Commander, U.S. Cyber Command, Director, NSA/Chief, CSS, partnered with the CCC to host a week-long session for a group of female college students interested in STEM careers. As part of "Women Immersed In NSA Cybersecurity," or WIN-Cyber, the students learned about NSA's different cybersecurity focuses and had the opportunity to see themselves at NSA.

Since March, the CCC has publicly released nine "Look Around: Women in Cybersecurity" videos that highlight women excelling in cybersecurity careers across the Intelligence Community. This not only highlights those already in the field, but encourages more women to join. NSA remains committed to ensuring all people see themselves in cyber

> By prioritizing diversity and investing in cybersecurity education from kindergarten through college, we are fostering the talent we need to tackle the difficult challenges of today and tomorrow.
>
> Dave Luber, NSA Cybersecurity Deputy Director

LOOK AROUND

Visit NSA's YouTube channel to watch the series "Look Around: Women in Cybersecurity." Hosted by CCC Chief Morgan Adamski, the short videos profile female cybersecurity leaders across the Intelligence Community.

CINDY WALSH-LEMLE
Chief Operations Officer,
NSA Cybersecurity Collaboration Center

Morgan Adamski, Cybersecurity Collaboration Center Chief, speaks to students at the “Women Immersed in NSA Cybersecurity” event.

NSA remains committed to ensuring all people see themselves in cyber and to fostering a diverse workforce that is reflective of the global community.

and to fostering a diverse workforce that is reflective of the global community.

PROMOTING DIVERSITY

NSA Cybersecurity Director Rob Joyce is a strong proponent for increasing diversity in the cybersecurity field. In February, he participated in a roundtable discussion with members of the #ShareTheMicInCyber movement, which aims to address issues stemming from systemic racism in cybersecurity. They discussed diversity and inclusion at NSA and some of the biggest cybersecurity challenges his teams face each day. He also sponsored and participated in a visit with members of Black Girls in Cyber non-profit, who discussed their careers and their efforts to promote diversity in cybersecurity.

EQUIPPING OUR SERVICE MEMBERS

Over 260 cadets and midshipmen from the U.S. service academies and the U.S. senior military colleges participated in the 2022 virtual NSA Cyber Exercise (NCX). The three-day event advances cybersecurity skills by developing and testing the talent, teamwork, planning, communication, and decision-making skills of future military leaders and cybersecurity professionals. Throughout the final cyber combat exercise, teams solved tasks and challenges while simultaneously offensively attacking and defending against

NSA and Georgia Tech leadership pose with the winners of the 2021 Codebreaker Challenge during a ceremony in Atlanta.

THE NSA CODEBREAKER CHALLENGE

Each year, students attending U.S.-based academic institutions are given the chance to sharpen their skills and gain experience in mission-centric scenarios similar to what the NSA workforce faces daily. Through December 31, students are taking on a ransomware attack challenge that gradually increases in complexity and tests their investigative skills. They must discover the tools and techniques used in the attack, unravel and expose a ransomware-as-a-service ring, and recover the critical files to save the day.

Initially launched in 2013 with just five participating schools, more than 5,400 students from 631 schools participated in the 2021 challenge. Colleges and universities have even incorporated the challenge into their curriculum, promoting intercampus engagement and strengthening U.S. cybersecurity education nationwide.

GENCYBER

NSA and the National Science Foundation fund camps and programs for students and teachers that increase awareness of K-12 educational cybersecurity content and cybersecurity postsecondary and career opportunities. In 2022, 74 schools across 37 states and the District of Columbia hosted student, teacher, and combination programs, as well as outreach/capacity building activities. To account for COVID-19, GenCyber provided hybrid (virtual and in-person) options.

other teams. The U.S. Air Force was awarded the 2022 NCX trophy.

Along with hosting the annual exercise, NSA also invites our nation's future military leaders for a hands-on tour at NSA. Nearly 150 cadets, midshipmen and students from across the U.S. service academies, Army Reserve Officers Training Corps (ROTC), and senior military colleges participated in the NSA Experiential Tour (NET). The offering educates service members about NSA's signals intelligence and cybersecurity missions so that they can apply this knowledge as they assume future military leadership roles in the extended cryptologic enterprise.

In 2022, the NET assigned ROTC cadets to the Johns Hopkins University Applied Physics Lab's CIRCUIT program where they piloted an unclassified critical thinking approach to address unique intelligence problems throughout the Intelligence Community.

EMPOWERING STUDENTS AND TEACHERS

NSA plays an important part in promoting cybersecurity careers and in developing professionals fit to take on an increasingly challenging cyber landscape. NSA's National Cryptologic University runs the National Centers of Academic Excellence in Cybersecurity (NCAE-C) program, which works with community colleges, colleges, and universities interested in advancing the study of cybersecurity. The program:

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

Nearly 400 schools have received the coveted NCAE-C designation in the areas of cyber defense, research, and operations. NSA has also validated nearly 500 programs of study. The Candidates Program boosted designations in 2022 by hosting workshops, seminars, and mentoring sessions with academic officials pursuing the NCAE-C designation for their schools. Application acceptance rates have risen 50 percent as a result of the program.