



Homeland  
Security

NATIONAL CYBERSECURITY  
AND COMMUNICATIONS  
INTEGRATION CENTER

## TABLE OF CONTENTS

	A Letter to Our Partners	1
	A Conversation with NCCIC Director John Felker	3
	Our Purpose: Driving Toward A More Secure Cyber and Communications Ecosystem	5
	Leading A Global Fight, Coordinating A Unified National Effort	11
	What We Do	17
	Evolving to Serve Customers Better: FY 2018 and Beyond	31
	Conclusion	35
	Appendix A: NCCIC Services	37

# A LETTER TO OUR PARTNERS

Fiscal Year 2017 was both eventful and exciting for the National Cybersecurity and Communications Integration Center (NCCIC). Throughout the year, we were reminded all too frequently that threats to the Nation's information and communications systems remain persistent and extremely dangerous. Yet there is also room for excitement and optimism because, while much work remains, NCCIC and our partners made real progress toward creating a more sustainable, secure, and resilient cyber and communications environment.

This *Fiscal Year 2017 NCCIC Year in Review* highlights NCCIC's important role in protecting the Nation's critical information and communications systems.

Misuse of, threats to, and malicious attacks on these systems pose some of the most serious and enduring strategic risks to the United States. The increasing frequency and scale of malicious cyber activity threatens us all. As more devices connect to the Internet, the threat landscape broadens and compounds the challenge for security practitioners.

NCCIC spearheads the Department of Homeland Security's operational efforts to reduce systemic risk to our information technology and operational technology (IT and OT), while

combatting persistent threats from sophisticated adversaries seeking to compromise our national security. Whether working with partners to tackle large-scale, global cyber attacks such as WannaCry and NotPetya, or coordinating the restoration of vital telecommunications in the wake of Hurricanes Harvey, Irma, and Maria, NCCIC is there to help the Nation prepare for, prevent, protect, and if necessary respond to incidents.

No one agency or organization can secure our homeland alone, however. Cyber and communications security is a shared responsibility. All of us, from the biggest government agencies and multinational corporations, to individual citizens play a part in keeping the Internet safe. Together, we can improve our collective defense through collaborative, tangible actions that make the cyber ecosystem safer. NCCIC's goal is a cyber environment where a given tactic, such as a malicious email, can only be used once before all other potential victims block it.

In FY17, NCCIC streamlined its product portfolio, further integrated core functions and capabilities, and improved services to customers in a number of important ways. We continue to explore ways to enrich cyber threat indicator data and leverage analytics and automation to improve the information we deliver to customers. We are also helping customers improve readiness and technical expertise by enhancing our training and exercise capabilities. These and other enhancements—together with the growing strength and breadth of our global partnerships—will help to



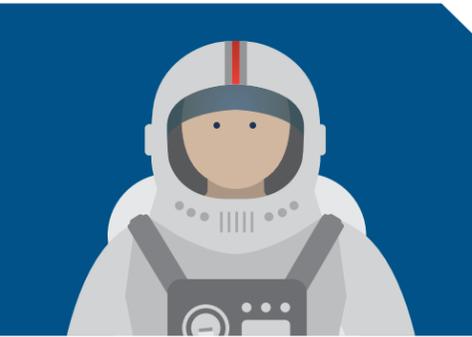
ensure that the NCCIC continues to arm our customers with the critical information products, services, and capabilities they require.

I want to thank our partners and the dedicated and skilled NCCIC team for their tireless work and contributions to the Nation's security.

Sincerely,

**Jeanette Manfra**

*Assistant Secretary for Cybersecurity  
and Communications*



# A CONVERSATION WITH NCCIC DIRECTOR JOHN FELKER

DHS established NCCIC in 2009. The National Cybersecurity Protection Act of 2014 (NCPA) established NCCIC in law. Together, NCPA and the Cybersecurity Act of 2015 collectively tasked NCCIC with a number of core cybersecurity functions, including serving as a federal-civilian interface for sharing cyber threat indicators, coordinating information exchange across the Federal Government, and providing information and recommendations on security and resilience measures to federal and non-federal entities.

## Q: What does NCCIC do?

NCCIC helps people and organizations defend their cyber and communications networks, and responds to nationally significant incidents when they occur.

We enhance the security of the cyber and communications ecosystem through threat information sharing across the globe. If reliable information flows quickly and to enough people, we can halt cyber incidents before they spread widely and cause significant harm. On our 24/7 watch floor, we continuously monitor national and international incidents and events that may affect cyber and communications infrastructure. By fusing information from all levels of government, the private sector, international partners, and the public, we help people and organizations take action to protect against cybersecurity risks. This coordination also improves government-wide incident and emergency response capabilities and strengthens resilience.

NCCIC's priority is delivering products and services to protect the networks and systems that underpin our Nation's critical infrastructure (CI). CI includes essential government services, financial institutions, energy providers, transportation systems, water treatment systems, public health, chemical and nuclear plants, and emergency services (table 1 shows the 16 identified CI sectors). At the same time, we make many of NCCIC's products and services available at no cost to all Americans to use to protect themselves from cyber threats.

## Q: How does NCCIC protect the public and private sectors from cybersecurity and communications threats?

Integration is one of our core functions. Many of our partners—including members of the intelligence community, law enforcement, and major Internet service providers—are co-located on our watch floor, which facilitates coordination and collaboration. We exchange information with these partners, analyze data, and provide results in publicly available alerts, technical advisories, and reports.

We also help stakeholders improve cyber hygiene, assess cybersecurity posture, test network defenses, and enhance preparedness and expertise through exercises and training. Additionally, when major incidents occur, the NCCIC team provides both remote and on-site incident response support to federal departments and agencies; state, local, tribal, and territorial (SLTT) governments; and the private sector.

## Q: What did NCCIC accomplish in Fiscal Year 2017?

As you will read throughout this report, NCCIC continued to operate at a high tempo in Fiscal Year 2017 (FY17). We responded to diverse incidents, conducted exercises to support operational readiness, and provided guidance on advanced persistent threat (APT) campaigns, including GRIZZLY STEPPE, Dragonfly, and HIDDEN COBRA.<sup>2</sup> In FY17, NCCIC also responded to malware implants on critical systems, including IT service providers, where an attacker could exploit credential compromises to gain access to customer network environments.

Working with our partners, we used our telecommunications capabilities to respond to major hurricanes, wildfires, and other natural disasters. We streamlined our cyber assessment and analytic teams to better enable network defenders to identify—and reduce the risk of—malicious attacks. We built out our vulnerability management capabilities to ensure responsible disclosure of IT and OT vulnerabilities and to provide corresponding research and analysis. We continued to develop and expand our capacity to respond to incidents, and we stood up a new cyber hunt capability that significantly improves our ability to proactively find threat actors on government and CI networks.

## Q: How is NCCIC evolving?

Our evolution is an ongoing process. We continuously look for ways to create a more nimble organization that can quickly adapt to the changing threat environment and deliver critical products and services to our stakeholders with greater speed,

value, and proficiency. We are just getting started, and the changes we are making are streamlining NCCIC operations, and improving analytical insight, information sharing, and response synchronization. As part of an internal realignment, we are organizing to more effectively deliver the products and services our stakeholders rely upon. We are bringing focus to cooperative efforts across the Office of Cybersecurity and Communications<sup>3</sup> (CS&C) to deliver a wide range of cyber and communications support functions.

To succeed in an ever-changing cyber and communications environment, we recognize that we must do an extraordinary job. We must always strive to be more effective in everything we do. We will continue to listen to our partners and stakeholders, learn from the evolving landscape, and adapt our operations and tools to be a step ahead of cyber threat actors.

## Presidential Policy Directive 21: Critical Infrastructure Security and Resilience

Designated Critical Infrastructure (CI) Sectors<sup>1</sup>

 <b>CHEMICAL</b> DEPARTMENT OF HOMELAND SECURITY	 <b>EMERGENCY SERVICES</b> DEPARTMENT OF HOMELAND SECURITY	 <b>HEALTHCARE AND PUBLIC HEALTH</b> DEPARTMENT OF HEALTH AND HUMAN SERVICES
 <b>COMMERCIAL FACILITIES</b> DEPARTMENT OF HOMELAND SECURITY	 <b>ENERGY</b> DEPARTMENT OF ENERGY	 <b>INFORMATION TECHNOLOGY</b> DEPARTMENT OF HOMELAND SECURITY
 <b>COMMUNICATIONS</b> DEPARTMENT OF HOMELAND SECURITY	 <b>FINANCIAL SERVICES</b> DEPARTMENT OF TREASURY	 <b>NUCLEAR REACTORS, MATERIALS, AND WASTE</b> DEPARTMENT OF HOMELAND SECURITY
 <b>CRITICAL MANUFACTURING</b> DEPARTMENT OF HOMELAND SECURITY	 <b>FOOD AND AGRICULTURE</b> DEPARTMENT OF AGRICULTURE, DEPARTMENT OF HEALTH AND HUMAN SERVICES	 <b>TRANSPORTATION SYSTEMS</b> DEPARTMENT OF HOMELAND SECURITY, DEPARTMENT OF TRANSPORTATION
 <b>DAMS</b> DEPARTMENT OF HOMELAND SECURITY	 <b>GOVERNMENT FACILITIES</b> DEPARTMENT OF HOMELAND SECURITY, GENERAL SERVICES ADMINISTRATION	 <b>WATER AND WASTEWATER SYSTEMS</b> ENVIRONMENTAL PROTECTION AGENCY
 <b>DEFENSE INDUSTRIAL BASE</b> DEPARTMENT OF DEFENSE		

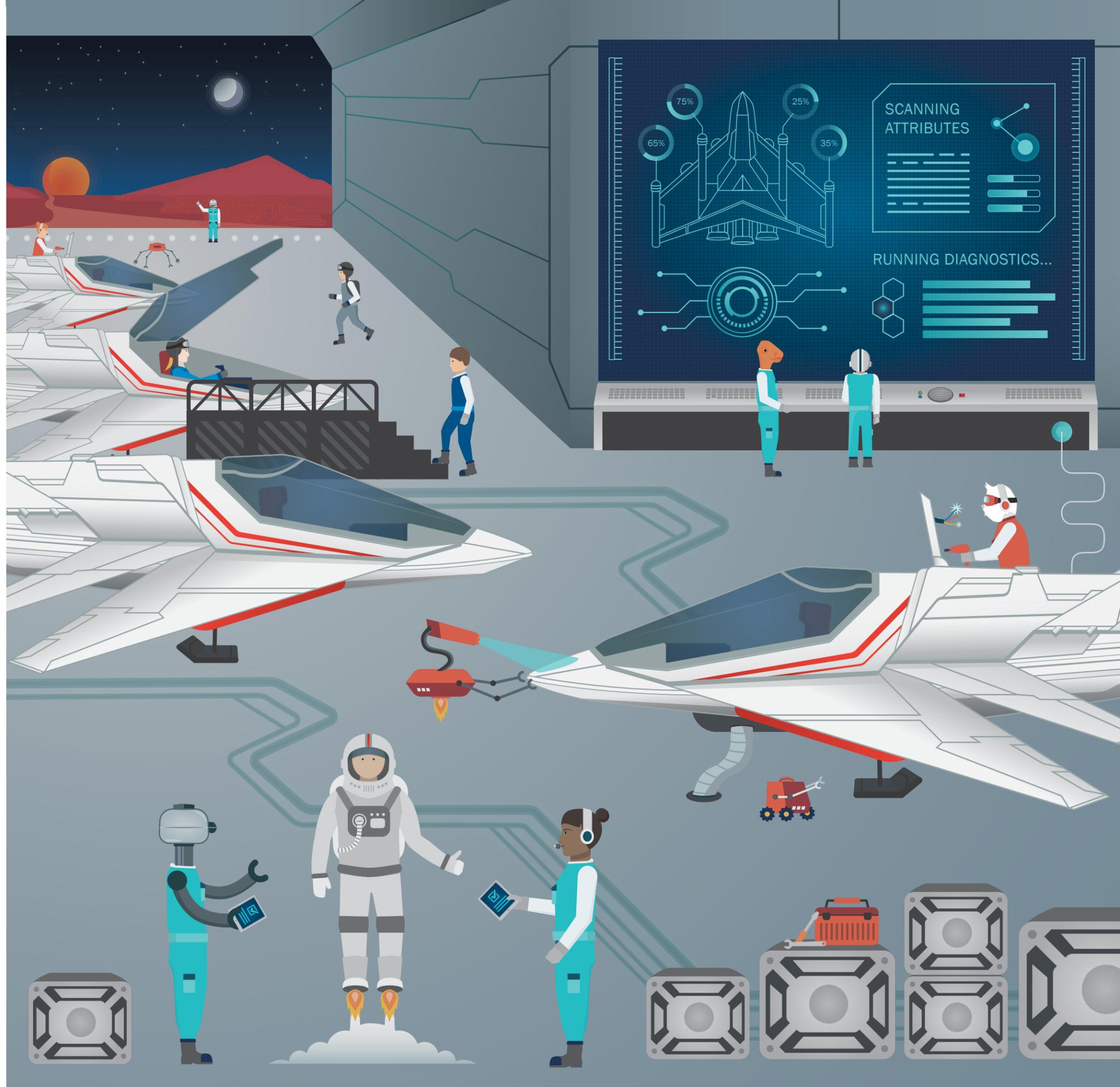
<sup>1</sup> Presidential Policy Directive-21: Critical Infrastructure Security and Resilience, establishes national policy on CI security and resilience. PPD-21 defines CI as systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. PPD-21 identifies 16 CI sectors and designates associated Federal Sector-Specific Agencies (SSAs) to lead Federal Government efforts to collaborate, coordinate, and implement actions to enhance the security and resilience of their respective CI sector.

<sup>2</sup> GRIZZLY STEPPE, Dragonfly, and HIDDEN COBRA are separate APT campaigns. Please visit <https://www.us-cert.gov> for more information.

<sup>3</sup> NCCIC is one of five CS&C divisions. The other divisions are the Federal Network Resilience Division, Network Security Deployment Division, the Office of Emergency Communications, and the Stakeholder Engagement and Cyber Infrastructure Resilience Division. CS&C is a component of DHS' National Protection and Programs Directorate, which is charged with leading the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure.

# OUR PURPOSE: DRIVING TOWARD A MORE SECURE CYBER AND COMMUNICATIONS ECOSYSTEM

NCCIC serves as the focal point for collaborative efforts between the public and private sector to facilitate threat information sharing across the globe. In everything we do, we follow a single-minded goal: help the Nation build a more secure and resilient cyber and communications environment.



# TIMELINE OF NCCIC HISTORY

436.243 million star units  
a: 8472846.0482  
b: 3573349.9573

316.243 million star units  
a: 334846.0482  
b: 535739.9573

136.243 million star units  
a: 8472846.0482  
b: 3573349.9573

236.243 million star units  
a: 234846.0482  
b: 535739.9573

**NCS**  
**1963:**  
Presidential Memorandum established the National Communications System (NCS)

**NCC**  
**1984:**  
Executive Order 12472 expands NCS to include National Security and Emergency Preparedness (NS/EP) and establishes the National Coordinating Center (NCC) for communications

**US-CERT**  
**2000:**  
Congress Created Federal Computer Incident Response Center (FedCIRC) at GSA to handle growing number of cyber breaches

**ICS-CERT**  
**2003:**  
Congress moves FedCIRC to newly formed DHS; renames as US-CERT and expands the mission to include cybersecurity

**2004:**  
DHS establishes the Control Systems Security Program (CSSP)

**NCCIC**  
**October 2009:**  
DHS establishes the NCCIC

**DHS**  
**2002:**  
DHS established by the Homeland Security Act

**2000:**  
the White House officially designates NCC as the Information Sharing and Analysis Center (ISAC) for Telecommunications

**2003:**  
NCS moves from the DOD to DHS

**2009:**  
National Security Telecommunications Advisory Committee (NSTAC) recommends establishing joint collaboration center that becomes basis for NCCIC

**2012:**  
Executive Order 13618 disbands the National Communications System (NCS); NCC assumes these new responsibilities

**2012:**  
DHS establishes ICS-CERT, replacing CSSP

**2012:**  
NCCIC co-locates US-CERT, ICS-CERT, and NCC into NCCIC watch floor

**2017:**  
DHS streamlines organizational structure, moving US-CERT, ICS-CERT, and NCC into a single NCCIC organizational structure

**2015:**  
The Cybersecurity Act of 2015 designates NCCIC as the central hub for cyber threat indicator sharing between government and the private sector



## OUR ORGANIZATION

As part of our commitment to serve customers better, over the last year NCCIC conducted an extensive internal review of operations. Based in part on the review, we created significant functional enhancements that position NCCIC as a more efficient and responsive organization. Specifically, these changes

- improve our overall analytic capacity and realign resources toward greater effectiveness;
- expand our incident response and tailored hunt services;
- integrate our information technology and operational technology (IT and OT) assessment and vulnerability coordination capabilities; and
- consolidate our national exercise and training programs.

The realignment integrates the United States Computer Emergency Readiness Team (US-CERT) and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) into a single, functionally organized NCCIC structure that combines intersecting functions from those legacy organizations. The work US-CERT and ICS-CERT performed as organizations under the NCCIC umbrella was extraordinary, and NCCIC retains all of the expertise, functions, and capabilities that those organizations provided. The dedicated professionals with whom our stakeholders have developed trusted working relationships will continue their specialized work within the NCCIC, ready to draw on the broader resources of the entire NCCIC to serve customers better.

Moving forward, our focus is on innovation, value, execution, and operational excellence. We will consistently look for ways to better serve stakeholders as together we build a more sustainable, secure, and resilient cyber and communications environment.

## OUR VISION

NCCIC's vision is a secure and robust cyber and communications infrastructure, resilient against attacks and disruption. In pursuing our vision, we adhere to a number of Guiding Principles:

- **Put Customers First.** Understand and meet our customer and constituent needs quickly and completely.
- **Lead the Global Mission.** In service to our national interests, serve as a global ambassador for cyber and communications security expertise, excellence, and information.
- **Be an Active Force for Good.** Defend the homeland by being the first and best option to identify, understand, prevent, protect, and respond to significant threats and exploitations of our cyber and communications infrastructure.
- **Drive Innovation.** Stay on the cutting edge of innovation to bring down risk, learning from past experiences and anticipating change. Inspire others to better understand and apply cyber and communications knowledge and tools.
- **Be Right, Be Fast.** Connect people-to-people and people-to-content to build community knowledge. Share threat and vulnerability information quickly and broadly, while maintaining the confidence and trust of our stakeholders, and the constitutional rights of the American people.
- **Earn Trust.** Relentlessly build our reputation as the authoritative source of information and a dependable partner, through technical excellence and accurate, timely analysis. We are the experts other professionals turn to for help.

## OUR MISSION

NCCIC's mission is to reduce the risk of systemic cybersecurity and communications challenges in our role as the Nation's flagship cyber defense, incident response, and operational integration center.

We execute this mission by serving as a national hub for cyber and communications information, technical expertise, and operational integration, and by operating our 24/7 situational awareness, analysis, and incident response center.

To execute its mission, NCCIC performs a number of core functions:

- **information exchange,**
- **training and exercises,**
- **risk and vulnerability assessments,**
- **data synthesis and analysis,**
- **operational planning and coordination,**
- **watch operations, and**
- **incident response and recovery.**

# LEADING A GLOBAL FIGHT, COORDINATING A UNIFIED NATIONAL EFFORT

NCCIC's mission can only succeed with the help and active participation of our stakeholders. We are committed to dialogue and engagement at all levels, whether it is operational coordination on the NCCIC watch floor, analyst-to-analyst exchanges, participation in industry events and global forums, or leading national-level cyber exercises. Trust within the community of cyber and communications stakeholders is essential to this collective defense strategy. NCCIC builds trust by:

- embedding confidentiality, privacy, and civil liberties protections into our information sharing culture;
- demonstrating our technical competence; and
- listening and responding to stakeholder needs.

NCCIC's primary stakeholders—customers, constituents, and partners—include the Federal Government; SLTT governments; private sector businesses (particularly those that manage critical infrastructure); the research and academic community; the public; and our international allies. Going forward, we will focus on new ways of adding value to our partnerships, and expanding the community of contributors to the global cyber and communications security mission.



## FEDERAL DEPARTMENTS AND AGENCIES

Federal network defense is a coordinated effort, and NCCIC collaborates closely with its constituent departments and agencies to help them take action to mitigate cyber risk.

Federal departments and agencies are also major contributors to our cyber and communications security capabilities. NCCIC coordinates with various federal organizations—particularly Sector-Specific Agencies, the Office of Management and Budget, other DHS organizations, and the intelligence and law enforcement communities—on a broad range of operational activities. For example, we maintain close operational relationships with other federal cybersecurity centers and federal security operations centers (SOCs). These include the following:

- Cyber Threat Intelligence Integration Center (Office of the Director of National Intelligence)
- U.S. Cyber Command Joint Operations Center (Department of Defense);
- Department of Defense Cyber Crime Center (DC3);
- National Cyber Investigative Joint Task Force (Federal Bureau of Investigation);
- Intelligence Community-Security Coordination Center;
- National Security Agency (NSA) Central Security Service Threat Operations Center; and
- various federal SOCs (e.g., Transportation Security Administration SOC).

During major incidents, or in response to sustained cyber campaigns and challenges, NCCIC spearheads DHS coordination and

collaboration with departments and agencies.<sup>4</sup> We provide situational awareness and advice to DHS leadership and senior government officials, Congress, and the National Security Council.

NCCIC also plays a key role in the Continuity Communications Manager's Group (CCMG) forum. Meeting every quarter, CCMG provides a critical forum for information sharing and coordination among continuity communications managers to address issues, challenges, opportunities, new technologies, and solutions. CCMG also addresses matters related to policy, planning, operations, testing, evaluation, and systems interoperability affecting the executive branch continuity communications environment. It is also an important forum to review and address continuity communications test results, trends, compliance assessment reports, and long-term communications challenges.

## PRIVATE SECTOR

The private sector owns and operates the majority of the Nation's critical infrastructure (CI), including "lifeline" sectors—Communications, Emergency Services, Energy, Transportation Systems, and Water and Wastewater Systems. Private sector organizations are essential

### ICSJWG: Uniting to Enhance ICS Security

In 2009, DHS established the Industrial Control Systems Joint Working Group (ICSJWG) to improve coordination and information exchange between government and the control systems community. ICSJWG is an essential platform for dialogue and collaborative action between NCCIC's industrial control systems (ICS) specialists and the ICS community.

Fostering the exchange of technical expertise and security awareness information between government and the ICS community, ICSJWG is one of NCCIC's most important and enduring partnerships. Members include ICS vendors and integrators, CI owners and operators, researchers, international partners, and federal departments and agencies.

Each year, ICSJWG holds spring and fall meetings. In FY17, 638 people attended the meetings, which included vendor expos, a two-day "hands-on" ICS workshop, and technical presentations on topics as diverse as ransomware, supply chain security, and meeting the demand for cybersecurity professionals.

partners. NCCIC needs private sector information, innovation, technical expertise, and active engagement to successfully carry out our mission. Additionally, our adversaries frequently target private sector CI organizations due to the degree to which society relies on the goods and services they provide. Because of this, private sector CI owners and operators are major consumers of NCCIC products, as well as essential partners.

NCCIC continues to integrate the private sector to better facilitate information flow during both normal and incident conditions. For example, we regularly work with CI partners on joint incident management actions and analysis to share with the broader CI community. The private sector organizations NCCIC engages include

- businesses of all sizes;
- vendors;
- researchers;
- universities;
- think tanks;
- industry associations;
- presidential advisory bodies;
- CI coordinating organizations; and
- individual CI owners and operators from across private industry.

## TELECOMMUNICATIONS INFORMATION SHARING

As part of our robust cyber collaboration with the private sector, we maintain close coordination with the telecommunications industry. In particular, NCCIC's National Coordinating Center for Communications (NCC) manages the Communications Information Sharing and Analysis Center (Comms-ISAC) to share and apply the technical expertise, threat awareness, and operational capabilities required to address hazards and risks to the Nation's telecommunications infrastructure. We maintain integrated operational relationships—physically and virtually—with communications service providers and other stakeholders to get real-time operating status and to coordinate assistance during an incident.

## STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENTS

State, local, tribal, and territorial governments, (SLTT) and regional organizations and officials are critical to the Nation's cyber and communications security. These include state Homeland Security Advisors, Chief Information Officers, Chief Information Security Officers (CISOs), intelligence fusion centers, law enforcement, community leaders, and emergency responders.

NCCIC coordinates closely with the Federal Emergency Management Agency (FEMA) and SLTT governments to support the restoration of communications infrastructure during major emergencies. NCCIC also works with SLTT partners to address communications threats facing public safety answering points (e.g., telephony denial-of-service attacks).

The Multi-State Information Sharing and Analysis Center<sup>5</sup> (MS-ISAC) is a critical state and local resource. Funded in part by DHS, MS-ISAC is an essential mechanism for coordination between NCCIC and SLTT customers. With dedicated liaison staff on the NCCIC watch floor, MS-ISAC is a focal point for state-level cyber threat prevention, protection, response, and recovery. As NCCIC receives information, MS-ISAC can quickly share that information with its members.

In late FY17, DHS added the Election Infrastructure (EI) Subsector to the Government Facilities Sector. NCCIC is an active participant and key member of the cybersecurity task force that supports the EI Subsector, helping to ensure the integrity and reliability of our critical election systems.

## Supporting Our Election Infrastructure

NCCIC was a critical contributor to a DHS initiative to ensure the integrity of the Nation's EI in preparation for the November 2016 general election. The purpose of the initiative was to raise awareness of cybersecurity vulnerabilities within voting infrastructure and increase the security and resilience of the electoral process.

Voting-related processes potentially at risk include electronic voting, Internet voting, and voter registration systems. NCCIC provided state and local governments—upon request—with free and continuous cyber hygiene scanning services, as well as in-depth vulnerability assessments of computer-enabled election systems. Since Fall 2016, more than 60 state and local jurisdictions have engaged NCCIC and signed up for continuous scanning and vulnerability assessment services.

In January 2017, DHS announced that election infrastructure would be a priority for cybersecurity assistance and protections on a formal and enduring basis. The designation of EI as a subsector of CI means that customers who request DHS services can now receive prioritized access to the full scope of NCCIC cybersecurity services.

Since September 2017, NCCIC has participated in the newly formed DHS Election Task Force. The task force supports information sharing on cyber threats with state election officials to help ensure the security and integrity of EI. In FY17, NCCIC worked with seven states and four local jurisdictions to conduct in-depth risk and vulnerability assessments to ensure the security and resilience of election systems for 2018 state and local elections. NCCIC will prioritize requests from SLTT partners—expected to increase as the 2018 elections approach—to ensure preparation for upcoming elections.

### Delivering End-to-End Services: City of Los Angeles Cybersecurity Engagements

NCCIC's work with the government of the City of Los Angeles is an excellent example of the end-to-end services we provide to help organizations reduce risk.

For example, NCCIC enrolled the City in the AIS initiative to enable automated sharing of cyber threat indicators of compromise (IOCs). We performed cyber hygiene vulnerability scans of key public-facing information systems and conducted cyber resilience reviews.

NCCIC also facilitated a cyber tabletop exercise at the U.S. Secret Service Los Angeles field office. The exercise tested citywide cybersecurity governance, with a focus on information exchange and cyber incident response plans and processes. The eight-hour exercise involved approximately 80 federal, state, and city participants and examined the City's ability to respond to a significant cyber incident affecting several of its departments.

The exercise clarified the primary and supporting roles and responsibilities of Federal, state, and local response entities.

<sup>4</sup> Presidential Policy Directive (PPD)-41, United States Cyber Incident Coordination, outlines the roles federal agencies play during a significant cyber incident. DHS plays a major role in both asset response and threat response. DHS is the lead agency for asset response during a significant cyber incident, focusing on the assets of the victim or potential targets of malicious activity. In fulfilling this responsibility, NCCIC assists asset owners in mitigating vulnerabilities, identifies other entities that may be at risk, and shares information across the public and private sectors to protect against similar incidents in the future. The Department of Justice, through the FBI and the National Cyber Investigative Joint Task Force, is the lead agency for threat response during a significant incident, with DHS's investigative agencies playing a crucial role in criminal investigations.

<sup>5</sup> Information Sharing and Analysis Organizations (ISAOs) seek to expand information sharing by encouraging the formation of communities that share information across a region or in response to a specific emerging cyber threat. Information Sharing and Analysis Centers (ISACs) are essential drivers of effective cybersecurity collaboration for specific industrial sectors such as banking and financial services, energy, telecommunications and defense. ISACs are trusted entities established by CI owners and operators to provide comprehensive sector analysis, which they share across sectors and with government.

## INTERNATIONAL PARTNERS

Cyber threats are borderless and ubiquitous. Attacks in distant parts of the world may replicate quickly and cause cascading consequences for our own cyber and communications infrastructure.

NCCIC is a leader in the global fight for secure cyber and communications networks, and brings together a broad range of international partners in a common effort to strengthen our capacity to fight threats. Through this work, we improve the cyber and communications risk posture of the United States.

Strengthening operational collaboration with international counterparts enables us to prepare for, prevent, mitigate, and respond to incidents that could degrade or overwhelm cyber and communications assets. Operational relationships among nations play a significant role in ensuring the safety and resilience of cyberspace. We know that our ability to respond to and overcome global cyber challenges improves in part by the degree to which we can act in close coordination and cooperation.

In close coordination with the State Department, NCCIC collaborates with international partners to build situational awareness, reduce risk, and coordinate information sharing and international response to incidents. We coordinate with our global peers in a number of areas, including

- exchange of technical expertise,
- threat intelligence sharing,
- establishing security standards,
- industrial control systems security, and
- cyber and communications capacity building.

We also participate in a range of multilateral and multi-stakeholder fora, including the following:

- Asia Pacific Economic Cooperation;
- Organization of American States;
- Organization of Economic Cooperation and Development;
- North Atlantic Treaty Organization (NATO);
- Organization for Security Cooperation in Europe;
- International Telecommunications Union Development Sector, Forum of Incident Response and Security Teams;
- Asia Pacific Computer Emergency Response Team; and
- Meridian Process and Conference.



## Fighting WannaCry Ransomware: A Sustained Global Effort

The May 2017 global WannaCry ransomware campaign highlights continued attempts by malicious actors to leverage cyberspace to disrupt international CI and cause economic loss. It is also an excellent example of how, together with our global partners, NCCIC can help fight such attacks and minimize their impact.

WannaCry began in Asia on May 12, 2017, and rapidly spread across the world—sources reported hundreds of thousands of infections in over 150 countries in just days. Due in part to the coordinated and sustained counteraction by NCCIC and its domestic and foreign partners, WannaCry had limited impact on U.S. CI.

WannaCry exploited a critical Windows Server Message Block vulnerability to remotely compromise victim systems, encrypt files, and spread to other hosts. Attackers demanded money to unencrypt the affected files.

As soon as WannaCry sightings were reported, NCCIC proactively began sharing information and coordinating with its international partners to understand and mitigate the impacts of the malware. NCCIC also worked with domestic security experts and researchers, and other federal departments and agencies. NCCIC's response included

- quickly sharing information that identified the vulnerability WannaCry exploited;
- conducting analysis on malware samples;
- issuing technical alerts identifying the indicators of compromise (IOCs);
- sharing the identified IOCs through AIS and the Cybersecurity Information Sharing and Collaboration Program (CISCP); and
- deploying signatures on EINSTEIN to protect federal networks.

NCCIC coordinated with more than 40 IT and cybersecurity companies (including major Internet service providers) to convey what we knew.

As part of its mission to protect federal departments and agencies, NCCIC also led Cybersecurity Coordination, Assessment, and Response (C-CAR) meetings to share actionable information about the threats. C-CARs are a critical complement to NCCIC's technical alerts and follow a standard protocol. This protocol enables DHS to convey information to CISOs and request action from federal departments and agencies to gain awareness of potentially affected systems across the Federal Government.

Recognizing that not all users would be able to install patches immediately, NCCIC also shared additional mitigation guidance to assist government and private sector network defenders.

The following timeline highlights key events in NCCIC's immediate response to WannaCry:

May 12, 2017	Open-source reporting on WannaCry ransomware began.
	NCCIC conducted malware analysis on multiple ransomware samples.
	NCCIC held cybersecurity coordination meetings.
	NCCIC published a Current Activity (CA): "Multiple Ransomware Infections Reported."
May 13, 2017	NCCIC published Technical Alert TA17-132A, "Indicators Associated with WannaCry Ransomware."
	NCCIC implemented Enhanced Coordination Procedures with cyber center partners to increase coordination and synchronization.
	NCCIC held coordination calls with over 40 IT and cybersecurity companies and all major ISPs to share known information and connect NCCIC operational teams with partners for analysis and information sharing.
May 14, 2017	A researcher identified a potential kill switch for the ransomware. NCCIC analysts corroborated that this kill switch stopped propagation of the ransomware.
	NCCIC became aware of additional variants of the ransomware.
May 15, 2017	The Small Business Administration posted DHS-provided information about the ransomware campaign to their website to assist small business owners.
	NCCIC released ICS-ALERT-17-135-01, "Indicators Associated with WannaCry Ransomware."
May 16, 2017	NCCIC posted ICS-ALERT-17-135-01 to its industrial control systems (ICS)-focused public website to raise awareness of the alert within the ICS community, and to identify affected ICS and medical device vendors.
	NCCIC posted Malware Initial Findings Report 10124171 – Ransomware/WannaCry and the associated technical indicators of compromise file to its website.
	CERT Europe (CERT-EU) distributed a revised WannaCry-related advisory that contained additional IOCs derived from the latest ransomware sample.
May 17, 2017	NCCIC conducted a data call to federal departments and agencies.
	NCCIC posted an ICS-CERT WannaCry fact sheet, "What is WannaCry/WanaCryptor?".
	NCCIC engaged department and agency security operation centers.

“ [Our IT and security company partners] stayed on the line with us, on these chat rooms and helped us pick [WannaCry] apart. And I really believe that that's the model for the future and it really just highlights all of the work that's gone on for years and years and years... just tremendous partnership and a [recognition] that we're all sort of in this together and we have to have that willingness [to work together]. ”

– Jeanette Manfra, DHS Assistant Secretary for Cybersecurity and Communications

# WHAT WE DO

Each day, NCCIC personnel work tirelessly to help our stakeholders secure their cyber and communications systems. Yet it is only with the enthusiastic participation of the entire cyber community that we will succeed in our mission. Our partners are essential to everything we do.



### NCCIC is a hub for information and expertise.

We are a global exchange for cyber and communications information, sharing what we receive back to the community.



Shared more than 15,600 alerts, bulletins, and other information products that raised security awareness and helped customers mitigate risk



Shared more than 3,000 indicators of compromise (IOCs) through the Enhanced Cybersecurity Services program and helped Internet service providers (ISPs) block malicious traffic for their customers



Received more than 727,000 reported cyber and communications threats



Grew Industrial Control Systems Joint Working Group to 2,680 members, expanding the collaborative community of industrial control systems (ICS) partners



Shared roughly 1.3 million IOCs since the inception of AIS in March 2016

### We build risk awareness and help people understand how to mitigate threats and vulnerabilities.

We help customers take action to improve their risk posture and support a common operational picture of the national cyber and communications risk landscape.



Detected more than 194,000 new vulnerabilities through cyber hygiene scans for hundreds of Federal Government customers



Completed 58 external exercises to build readiness and operational coordination among government and private sector customers



Trained more than 1,400 professionals in ICS security



Helped more than 2,100 customers use the Cybersecurity Evaluation Tool (CSET) to conduct self-evaluations of their ICS security posture



Conducted more than 160 on-site enterprise and control systems assessments to help customers understand and mitigate risk across all critical infrastructure (CI) sectors



Conducted 71 risk and vulnerability assessments for government and private sector clients

### We defend federal networks and respond to significant incidents.

Perhaps most importantly, we are here for our partners and customers when they need help. We vigilantly defend the Federal Government's critical networks and stand ready to respond to attacks on both government and private sector networks.



Provided on-site incident response support to roughly 30 government and private sector customers



Received roughly 106,000 incident reports from Federal and state, local, tribal, and territorial (SLTT) governments and the private sector, affecting communications, enterprise, and control systems



Detected 447 incidents through the EINSTEIN program, resulting in actions to secure federal networks



Helped customers mitigate roughly 225,000 vulnerabilities identified through cyber hygiene scans

## A GLOBAL FOCAL POINT FOR INFORMATION AND EXPERTISE

NCCIC uses information from across the globe to defend federal networks, to help the private sector defend its own networks, and to build community knowledge and current-state awareness of the cyber and communications risk landscape. NCCIC receives classified and unclassified information through trusted, operational relationships with a broad range of partners, including

- the intelligence community;
- law enforcement;
- states and localities;
- foreign governments;
- private companies;
- Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs);
- vendors and integrators;
- researchers; and
- other contributors such as non-governmental organizations.

We supplement this information with our own assessment, cyber hunt, network monitoring, threat and malware analysis, and open-source research activities.

### COMMS-ISAC: NCCIC's Partner in Information Sharing

A core contributor to this information sharing mission is the Communications ISAC (Comms-ISAC), managed by NCCIC's National Coordinating Center for Communications (NCC). The Comms-ISAC comprises communications service providers (CSPs)—including wireline, cellular, cable, satellite, and broadcast—equipment manufacturers, vendors, associations, and other industry partners. The Comms-ISAC facilitates the exchange of analyzed vulnerability, threat, intrusion, and anomaly information across the telecommunications community to help prevent, mitigate, respond to, and recover from communications threats and disruptions.

When our partners—both domestic and international—share information with us, we can share it with our stakeholders to enhance situational awareness and defense efforts across the globe. We regularly share alerts and warnings with international partners—through multilateral fora and bilateral relationships—so that they can better protect their infrastructure. NCCIC relies on the information received from these partners to inform our own cyber and communications security and resilience efforts.

## THE WATCH FLOOR: NCCIC'S INFORMATION SHARING HUB

Each day, NCCIC's 24/7 watch floor receives, triages, tracks, coordinates, and manages high volumes of threat, vulnerability, and incident information. The watch floor disseminates this information to NCCIC analysts for resolution and—as quickly as possible—shares alerts, reports, and other information products back to the community, so that our customers and partners can take action.

A diverse set of information sources is vital to developing a big-picture perspective of the Nation's systemic cyber and communications risk. In turn, this overarching view helps us “connect the dots,” so that we can quickly identify and help our customers mitigate threats and respond to incidents.

Operating in two physical locations—Arlington, VA, and Pensacola, FL—the watch floor provides shared national-level situational awareness and a forum for real-time operational collaboration with NCCIC's many partners. Our Arlington operations are co-located with the National Infrastructure Coordinating Center (NICC)<sup>6</sup> to ensure coordinated and consistent information exchange with our customers for both physical and cyber threats.

<sup>6</sup> NICC is the dedicated 24/7 coordination and information sharing operations center that maintains situational awareness of the Nation's critical infrastructure for the Federal Government.

## EXPANDING OUR INFORMATION SHARING CAPABILITIES

In addition to the watch floor, we share information through numerous additional methods, including automated machine-to-machine sharing in near real-time, cooperative agreements with private industry, vulnerability disclosure programs, and timely alerts and warnings.

Over the last year and a half, NCCIC expanded its information sharing capabilities in two important ways: we launched the Automated Indicator Sharing (AIS) initiative, and incorporated the Cybersecurity Information Sharing and Collaboration Program (CISCP) into NCCIC operations.

AIS automates the sharing of IOCs, creating an ecosystem where as soon as businesses or federal departments and agencies observe attempted compromises, they can share the IOCs in near real-time with the entire AIS community. AIS focuses on volume and velocity—not human validation of each IOC—and provides NCCIC partners with real-time data that enables them to take action against threats.

Similarly, CISCP enables private sector CI partners and NCCIC to exchange cyber threat, incident, and vulnerability information to support network defense. Through CISCP, participants receive NCCIC's in-depth analytical products that correlate detection and

defensive measures, as well as recommended practices focused on threat detection, prevention, and mitigation. CISCP also hosts analyst-to-analyst technical threat exchanges and analyst training events that include detailed threat briefings.

### Data Security: How We Safeguard Your Information

As a global information sharing hub, NCCIC bears a significant responsibility to protect the information we receive and to ensure we safeguard privacy, civil rights, and civil liberties. We take this responsibility extremely seriously and we do everything in our power to earn our stakeholders' trust by maintaining the confidentiality of sensitive information.

The Protected Critical Infrastructure Information (PCII) program is one significant way NCCIC ensures that critical infrastructure information stakeholders share remains protected from

- » the Freedom of Information Act (FOIA),
- » SLTT disclosure laws,
- » use in regulatory actions, and
- » use in civil litigation.

Only trained and certified federal, state, and local government employees or contractors may access PCII and only in accordance with strict safeguarding and handling requirements.

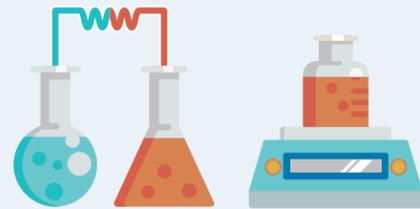
NCCIC also uses the Traffic Light Protocol (TLP) to safeguard information. TLP is a set of designations used to ensure that sensitive information is only shared with the appropriate audience. TLP is a simple, yet effective, schema that employs four colors to indicate when and how sensitive information can be shared, facilitating more frequent and effective collaboration.

In all instances, NCCIC prioritizes the security and privacy of information when sharing with its partners. For example, we limit IOC information to that necessary to characterize the threat. Another example of DHS's commitment to data protection is the Continuous Diagnostics and Mitigation (CDM) program. Through CDM, government entities can purchase cybersecurity services. CDM data feeds provide government-wide network visibility to NCCIC through a common dashboard. However, CDM's design also rigorously ensures data does not include any Personally Identifiable Information—information about specific user accounts.

## BUILDING UNDERSTANDING AND AWARENESS OF SYSTEMIC RISK

As attacks on our cyber and communications infrastructure grow in diversity, prevalence, and sophistication, NCCIC's mission demands that we stay ahead of the threat curve. One of the ways we do this is by synthesizing our data with data from open-source research, private sector partners, the intelligence community, international partners, and federal network feeds. The greater the volume of high-quality data NCCIC receives and analyzes, the better our understanding of threats and vulnerabilities.

Using this data, along with state-of-the-art tools and techniques, our analysts work to determine the nature of threats to systems, including enterprise business networks, control systems, and telecommunications infrastructure. They apply this knowledge to analytical offerings, which include technical alerts, guidance, best practices, and direct operational communication with other analysts in government and the private sector. These products integrate threat information, help provide an overall picture of the risk landscape, and support incident response.



### TECHNICAL ANALYSIS CAPABILITIES

Our technical analysis directly supports our mission to reduce risk to the Nation's CI. NCCIC technical analysts provide malware analysis, digital analysis, reverse engineering, and trend analysis. Their expertise and findings inform our exploration of systemic vulnerabilities; potential future threats; tactics, techniques, and procedures (TTPs); and more intractable long-term problems.

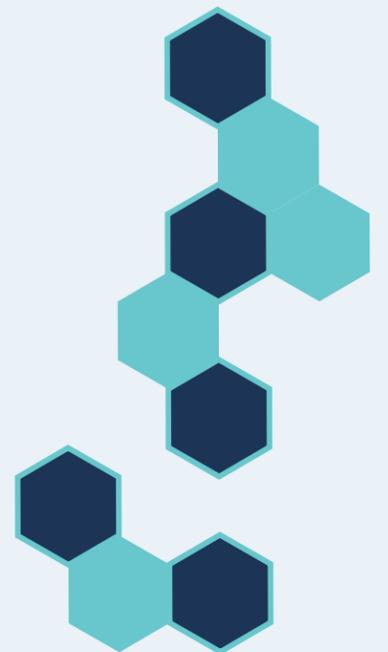
Our analysis and vulnerability coordination services reside primarily in our advanced malware analysis laboratories. We are increasing our focus on identifying trends and systemic risks associated with rapidly evolving areas such as the Internet of Things, including networked medical devices and avionics, cloud technologies, and the continued convergence of traditional telecommunications infrastructure with cyber-based technologies.

## Suspected Malware? Our Data Analysis Team Can Help

While not every detected malware instance is as damaging or far-reaching as WannaCry, all are worthy of NCCIC's attention and support. NCCIC's malware laboratories have a streamlined process to help network owners understand the risks associated with suspected malware activity. Network owners can submit files directly to NCCIC's malware analysis team for action through a secure web portal, email, or file transfer protocol.

Once received, NCCIC analysts review the files for IOCs to determine the type of malware potentially present. We provide the network owner with a report detailing the type of malware detected, an analysis of the IOCs present, and a list of appropriate mitigation strategies. NCCIC develops reports in several formats and specifications, including Structured Threat Information eXpression (STIX)—a standard language used to automate the exchange of cyber threat information.

A combination of open-source, commercial, and custom-developed tools power the malware analysis process. NCCIC analysts use automated toolsets to analyze malware, but also have the capability to reverse engineer malware files to gather information and develop associated IOCs. Analysts convert IOC information into anonymized, shareable reports to inform the larger cyber community. By sharing information of suspected malware with NCCIC, network operators can better secure their own network while reducing systemic risk across the entire cyber landscape.





## SUPPORTING RISK-BASED CYBERSECURITY: ASSESSMENTS AND CYBER HUNT

Our assessment and cyber hunt capabilities enable our customers to take a proactive, risk-based approach to cybersecurity, and to target specific improvements to their cyber risk posture.

NCCIC risk and vulnerability assessment services focus on analyzing customer networks to identify and help remediate weaknesses. They include highly automated cyber hygiene scans that help customers secure their network perimeter by assessing their Internet-accessible systems for known vulnerabilities and configuration errors. We conduct vulnerability scans, phishing campaign assessments, risk and vulnerability assessments, federal High Value Asset assessments, remote penetration testing, federal Red Team assessments, and operational assurance reviews.

FY17 also marked some innovative enhancements to our information technology (IT) and operational technology (OT) assessment capabilities. We integrated our end-to-end assessment service offerings for enterprise and ICS environments, providing a seamless assessment capability to customers. Most significantly,

we increased the number of assessment teams we can field, thereby expanding our capacity to serve both federal and private sector CI customers. We also added a new remote log analysis capability to our ICS assessment services. Our process now provides the NCCIC team with a better understanding of customer systems, and helps the customer identify and pull relevant log data in advance of the on-site assessment. In addition to facilitated assessments, we continue to offer the Cybersecurity Evaluation Tool (CSET)—a downloadable tool that enables CI owners and operators to conduct a self-assessment of their control systems networks.

NCCIC’s cyber hunt services, which we continue to expand, also provide customers greater visibility into the security posture of their networks. NCCIC conducts hunt missions at the invitation of government and private sector customers, including CI owners and operators. Hunt missions proactively search for malicious activity to help customers identify potential exploitation. NCCIC’s cyber hunt focuses on deep technical analysis of a live network with the intent of identifying previously unobserved threats.

## Trending System Vulnerabilities

Lapses in basic cybersecurity practices continue to be the most prevalent type of vulnerability our teams discover when assessing enterprise systems. As was the case in FY16, in FY17 our assessment teams found the most frequently identified enterprise system vulnerabilities to be

- » susceptibility to email phishing,
- » poor password practices,
- » poor patch management, and
- » improper configuration.

Within those categories, we have seen an increase in use of insecure default configurations and unsupported operating systems. On a positive note, we have also seen an overall decrease in reuse of administrator passwords as well as passwords stored in clear text.

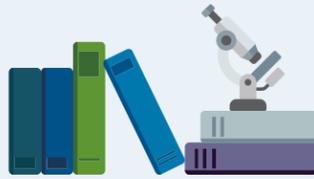
For Internet-facing systems, over half of the vulnerabilities we detected dealt with use of weak cipher suites within the Secure Socket Layer/Transport Layer Security protocol.

In FY17, our ICS assessment teams found the most frequently identified control system vulnerabilities to be

- » boundary protection—this was the single most prevalent area of concern, continuing a four-year trend,
- » identification and authentication of legitimate system users, and
- » allocation of resources.

Boundary protection is a critical element of defense-in-depth strategies—effective ICS defense requires a network architecture that isolates sensitive control systems from enterprise networks, which are inherently more risky. With respect to allocation of resources, NCCIC repeatedly found that ICS operators struggled with staff limitations when working to execute critical cybersecurity tasks.

## Assessment-to-Incident Response: Providing Fully Integrated Cybersecurity Services



In 2017, NCCIC performed 139 on-site ICS assessments to determine how well customers' cyber defenses could prevent malicious attacks. NCCIC assessments focus on identifying security gaps with the greatest potential for exploitation and harm, and on identifying and recommending solutions with the greatest benefit.

The teamwork and close collaboration between our assessment and response units is a good example of NCCIC's approach to customer service—we focus on providing customers with a fully integrated cybersecurity service portfolio to meet all their needs. When NCCIC responds to an incident, our response team often recommends that the affected organization undergo a full network assessment (after the response team resolves the immediate issue) to maximize overall network health and hygiene, and reduce the likelihood and severity of future incidents.

A recent routine assessment and analysis for a control systems customer in the Transportation Sector exemplifies the benefits of NCCIC's integrated customer service approach. During the assessment process, our assessors noted excessive Internet Control Message Protocol traffic originating from a control systems host that was communicating out to various Internet Protocol (IP) addresses around the world. This indicated potentially malicious activity, so NCCIC assessors immediately recommended involvement from NCCIC's incident response team.

At the asset owner's request, NCCIC switched its focus from an assessment to an incident investigation, and quickly discovered that the suspicious traffic was likely due to automated scanning of external IPs by the ICS host. Forensics analysis revealed the ICS host had been subjected to brute-force hacking attempts against its remote desktop service. The analysis also revealed that the remote desktop service was directly accessible from the Internet and not protected by a firewall or virtual private network. NCCIC provided mitigation guidance to the organization, which included establishing firewall protection to prevent unauthorized access from the Internet.

On federal networks, NCCIC cyber hunt teams search for malicious actors inside high-value assets (HVAs), and tailor assessments specifically to systems that connect to—or interact with—HVAs. These teams work closely with NCCIC HVA penetration testers.

NCCIC cyber hunt team services include

- examination of existing cybersecurity policies, procedures, and processes;
- system owner interviews;
- host-based analysis;
- review of existing logs;
- network traffic analysis; and
- data mappings and other diagrams.

NCCIC hunt teams use data drawn from the broad array of NCCIC sources—including the intelligence and law enforcement communities—to identify malicious tools and adversary TTPs extant on customer networks.

### BUILDING TECHNICAL EXPERTISE AND PREPAREDNESS: TRAINING AND EXERCISES

In FY17, NCCIC consolidated and integrated its technical training and exercise products and services to enhance the way we deliver these capabilities to our customers.

Our robust cyber exercise program enables government and private sector partners to plan and test their preparedness, policies, processes, and procedures when responding

to cyber and communications incidents. NCCIC offers a variety of scalable exercise formats—from facilitated, targeted attack tabletop discussions to full-scale, national-level functional exercises. Our services include the design, development, planning, evaluation, and conduct of cybersecurity exercises. These critical exercises enable us to provide insight into how our partners detect and respond to a variety of attacks and how they can further strengthen their defenses.

An important focus for our technical training is the planned expansion of our ICS training capabilities. Current training offerings include web-based and instructor-led technical training. As part of our advanced training course, NCCIC offers an advanced Red Team-Blue Team exercise within a simulated ICS training environment. In March 2017, NCCIC celebrated its 100th training class for Red-Blue Team training (formally known as the Industrial Control Systems Cybersecurity (301) Advanced Training). The training offers a hands-on approach to understanding a network environment, identifying potential vulnerabilities, evaluating exploitation of vulnerabilities, and applying defensive and mitigation strategies to protect industrial control systems. To date, more than 4,500 trainees have completed the training.

In 2017, NCCIC's Training team:

- conducted 12 ICS Red-Blue Team courses;
- led four regional sessions with introductory and intermediate content (three of which were for international partners);
- trained more than 1,200 students in instructor-led classes;
- conducted 17 tours of NCCIC's control systems analysis center in Idaho Falls, Idaho; and
- saw roughly 20,000 trainees complete one or more online classes.

## Cyber Guard and Cyber Storm: Preparing for National-Level Cyber Incidents

In FY17, NCCIC led DHS planning and coordination for Cyber Guard, an annual two-week exercise headed by Department of Defense (DOD) U.S. Cyber Command and co-sponsored by DHS and the Federal Bureau of Investigation (FBI).

Cyber Guard 2017 included experts from over 100 organizations, including the Federal Government, state governments, industry, academia, and international allies. Participants practiced tactical cyber incident response processes and operational coordination. NCCIC personnel participated at the main exercise location in Suffolk, VA, and from NCCIC's Pensacola, FL, location. Cyber Guard 2017 enabled NCCIC to hone incident response processes while also enhancing working relationships with partners who are pivotal to our ability to respond effectively to national-level cyber incidents.

In FY18, NCCIC will lead all aspects of Cyber Storm, a national-level exercise occurring every two years. Planning for Cyber Storm VI, slated to occur in Spring 2018, is already well underway.

Cyber Storm VI exercise will focus on the Critical Manufacturing and Transportation Sectors with participation from the Information Technology and Communications Sectors; law enforcement, defense, and intelligence agencies; state and local governments; and international partners.

We conducted Cyber Storm V in March 2016. The exercise focused on testing preparedness and response to a multi-sector cyber attack targeting the Healthcare and Public Health and Commercial Facilities Sectors. The exercise included more than 100 organizations and 1,200 players from across the globe. More than 96 percent of respondents to an after-action questionnaire indicated that participation in Cyber Storm V helped them become better prepared to deal successfully with a cyber incident.

### Building Global Expertise and Capacity

Cybersecurity is a global concern, and as our allies' cybersecurity capabilities grow, so does U.S. security. NCCIC works extensively with international partners to help them build cybersecurity technical expertise and understanding.

In July 2017, instructors from NCCIC's Training team traveled to Vilnius, Lithuania, to conduct an international training session on cybersecurity for industrial control systems (ICS) at the University of Lithuania's Faculty of Mathematics and Informatics.

The Lithuanian Ministry of Defense hosted the training in cooperation with U.S. European Command. More than 100 information technology specialists—working in various CI sectors in Lithuania and other NATO countries—attended the training. Represented countries included the Czech Republic, Denmark, Estonia, Germany, Latvia, Lithuania, Netherlands, Poland, the Slovak Republic, Slovenia, and the United States.

At the invitation of Japan's Ministry of Economy, Trade and Industry (METI) and the Information-Technology Promotion Agency, in September 2017, NCCIC also traveled to Tokyo, Japan, to participate in an ICS cybersecurity joint training.

This event, held at the Industrial Cybersecurity Center of Excellence in Tokyo, aimed to help combat Japan's shortfall of cybersecurity manpower. Representatives of METI stated that the training was very beneficial to students, not only enhancing their skills and knowledge relative to ICS, but also helping them learn of the advantages of global collaboration in cybersecurity.



## DEFENDING FEDERAL NETWORKS AND RESPONDING TO SIGNIFICANT INCIDENTS

One of our core mission areas is leading efforts to protect federal civilian government networks. Threat actors consider federal departments and agencies high-value targets, given the critical services they provide and the sensitive data they store. NCCIC provides federal partners with critical threat intelligence and network defense tools to enable them to effectively thwart cyber attacks. Additionally, NCCIC assists these partners with incident management and response.



## THE EINSTEIN PROGRAM

Through the National Cybersecurity Protection System, NCCIC uses EINSTEIN program outputs to support cyber defense of the Federal Government. EINSTEIN is a unique sensor grid that covers all federal department and agency civilian networks. It provides perimeter protection capabilities to help the Federal Government detect and block cyber threats. EINSTEIN sensors monitor and capture network data flows to and from federal systems, providing intrusion detection and prevention capabilities. NCCIC also analyzes sensor data to discover and track adversary TTPs, and to identify new IOCs. When necessary, NCCIC generates and disseminates alerts to help federal departments and agencies protect themselves from threats and vulnerabilities. NCCIC continues to implement tactics that strengthen government and the private sector network defense capabilities, such as

- increasing the number of IOCs that it shares,
- deploying “reputation scoring” to help organizations prioritize IOCs, and
- piloting advanced analytics to identify cyber threat patterns.

“The Department of Homeland Security, acting through the National Cybersecurity and Communications Integration Center,<sup>7</sup> shall be the Federal lead agency for asset response activities.”

—Presidential Policy Directive 41: United States Cyber Incident Coordination

## RESPONDING TO CYBER AND COMMUNICATIONS INCIDENTS

NCCIC focuses extensive resources on defending government networks and supporting private sector preparedness and protection.

The persistence, dynamism, and volume of attacks against IT and OT networks, however, combined with an ever-expanding attack surface as more devices connect to the Internet, means that some malicious attacks will inevitably succeed. In addition, 2017 was a stark reminder of the devastation that natural disasters can wreak on people, local and regional economies, and on our cyber and communications infrastructure. Responding to these events—and supporting our customers’ response—is a fundamental function that we continually strive to improve.

### Hunting for Malicious Activity

In 2017, NCCIC actively tracked, researched, and analyzed the technologies and methods cyber threat actors used to exploit vulnerabilities, and the behaviors of new or high-impact malware not attributed to a known adversary. Through these activities, NCCIC identified previously unrecognized threat actor TTPs. Based on these findings, NCCIC developed analytic products and reports, providing federal network defenders with the information necessary to understand adversary TTPs and reduce exposure to malicious activity.

### Augmenting Incident Response Resources

In FY17, NCCIC merged its ICS and enterprise response resources, augmenting our overall capabilities to meet increased customer demand and more efficiently deploy incident responders. This integration helps us meet the requirements of

- » Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,
- » the Cybersecurity Information Sharing Act of 2015, and
- » Presidential Policy Directive 41: U.S. Cyber Incident Coordination.

In FY18, we will continue to expand our ability to provide hunt services and on-site incident response to customers. We will also continue to mature our remote analysis capabilities, enabling incident responders to support a larger number of systems with existing resources.

NCCIC is the lead federal organization responsible for assisting victims in finding malicious activity on their systems in the wake of a “significant cyber incident.”<sup>7</sup> This includes leading remote and on-site responses to cyber attacks on federal networks. NCCIC also supports operational awareness and mitigation actions across the federal domain by using threat information detected in one department or agency to protect the rest of the government and to help the private sector protect itself.

During incidents and times of crisis, our operational planning and coordination team works across government to provide critical information and overarching context to inform the decisions of the White House and other government organizations. NCCIC works with affected government and—when requested—private sector stakeholders to help repair systems, patch vulnerabilities, reduce the risk of future incidents, and prevent an incident from spreading to others. Our incident response services include expert intrusion analysis and mitigation guidance to customers who require external assistance. While NCCIC prioritizes major cyber incidents that have the potential to disrupt or disable our CI, we offer stakeholders—including federal, SLTT governments, and private sector organizations—support for responding to minor incidents as well.

<sup>7</sup> Presidential Policy Directive 41: United States Cyber Incident Coordination, defines a significant cyber incident as an incident that is “likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.”

## Disaster Response: Restoring Critical Communications

In 2017, NCCIC led an extensive interagency effort to restore critical communications in the wake of four large-scale hurricanes that affected the lives of millions and devastated large areas of Florida, Georgia, Puerto Rico, Texas, and the U.S. Virgin Islands.

Through Emergency Support Function (ESF #2) – Communications<sup>8</sup>, NCCIC’s National Coordinating Center for Communications (NCC) coordinated federal interagency efforts to restore communications infrastructure; coordinated communications support to response efforts; facilitated the delivery of information to emergency management decision makers; and assisted in the stabilization and reestablishment of communications systems and applications.

ESF #2 members within DHS—alongside the Federal Communications Commission, the National Telecommunications and Information Administration, the General Services Administration, and the Department of Defense—supported response efforts to affected areas. Together, this interagency team

- ensured communications were available to impacted communities and responders;
- supported planning, including the development of a public safety recovery plan and integrated power-communications restoration plans; and
- acted as translators, radio operators, logisticians, and imagery analysts.

The team’s efforts supported the issuance of two communications-related executive orders in Puerto Rico, which enabled expedited communications restoration and waived taxes for communications equipment temporarily imported to restore communications. NCCIC also led the ESF in developing a plan to restore public safety land mobile radio communications in Puerto Rico. To improve customer connectivity, the interagency team leveraged partnerships in Puerto Rico and the U.S. Virgin Islands to increase roaming agreements.

As the national coordinator for ESF #2, NCCIC led efforts with industry partners in each of the affected states and territories to share resources and information to improve the ability of the Communications Sector to provide service to affected areas.

In the wake of each disaster, NCCIC and its partners joined in efforts to restore critical communications by helping to prioritize and resolve issues related to fuel, transportation, and access. NCCIC also helped forge an agreement—among carriers, tower owners, site owners, debris removal and road clearance teams, tower climbers, generator technicians, and fuel suppliers—to expedite site repair through prioritization and collaboration.

NCC also provided extensive analytical support to affected areas. This included

- over 100 telecommunications infrastructure analysis reports before and after hurricanes;
- coordination of the expedited delivery of 30,000 phone numbers needed to put replacement phones into service on the U.S. Virgin Islands, shrinking a multi-week process to days;
- deployment of more than 80 staff to assist affected areas in Florida, Georgia, Puerto Rico, Texas, the U.S. Virgin Islands, and FEMA Headquarters;
- daily reports and graphics providing overall telecommunications landline and cellular networks statistics for the affected areas;
- maps projecting cellular coverage of Puerto Rico at least three times a week, in coordination with the telecommunications carriers; and
- continuous updates to maps, identifying the availability and location of ancillary cellular equipment (such as hotspots, cell on wheels, and cell on light trucks).

NCCIC continues to work with its government and industry partners to prepare for communications disruptions through coordinated planning, exercises, and training.

<sup>8</sup> ESF #2 is the Communications Annex to the National Response Framework (<https://www.fema.gov/media-library/assets/documents/117791>). ESF #2 coordinates Federal actions to assist industry in restoring public communications infrastructure and to assist SLTT governments with emergency communications and the restoration of public safety communications systems and first responder networks. ESF #2 supports federal departments and agencies in procuring and coordinating National Security and Emergency Preparedness communications services. ESF #2 also addresses cybersecurity issues that result from or occur in conjunction with incidents. However, for incidents that are primarily cyber in nature, the Cyber Incident Annex is used and ESF #2 supports responses to cyber incidents as directed.

# The Future of NCCIC Information Sharing: Advancing Automated Indicator Sharing, Behavioral Analytics, and Orchestration



The launch of the DHS Automated Indicator Sharing (AIS) initiative in March 2016 marked a significant milestone in the government's use of automation to support cybersecurity. NCCIC continues to evolve indicator sharing and is building on the success of AIS to advance the sharing of actionable cybersecurity information through automation and behavioral analytics.

Through AIS, government and private sector participants exchange cyber threat indicators in near real-time. Threat indicators—also known as IOCs—are pieces of information, such as malicious IP addresses or malware hashes that may signify potential malicious activity. AIS shares as many IOCs as possible, as quickly as possible. Through rapid, high volume IOC sharing, AIS minimizes the number of times adversaries can use the same attack, raising the opportunity costs of the attack, and decreasing the overall cyber attack prevalence. There are now 184 government and private sector entities—covering all 16 CI sectors—connected to the AIS server. AIS has received and shared more than 1.4 million IOCs since its inception.

Mr. Preston Wertz oversees the implementation of AIS. He works within DHS and with government and private sector partners to explore how NCCIC can use technology to improve automated cybersecurity. Wertz sees AIS as an encouraging step in the right direction, while noting that NCCIC continues to look for ways to improve the initiative. "AIS is successful so far, but we recognize that we need to continue to explore ways to maximize its value," Wertz said. One way to increase the value of AIS is to expand coverage and participation. Strategic partners such as vendors, Information Sharing and Analysis Centers (ISACs), and Information Sharing and Analysis Organizations (ISAOs)—with broad customer or membership bases—can be highly effective force multipliers and significantly expand AIS participation.

NCCIC is also investigating ways to improve the operational relevance and quality of the IOCs it shares by adding context and correlation. This includes both technical context and intelligence context, such as the IOC's origination and whether

it comes from a sophisticated threat actor. To help provide this context, NCCIC is focusing on automated capture of IOC "sightings"—the number of times the community sees an IOC—and on identifying the IOCs that resulted in recipients taking action. "We want to know when organizations see content and take action based on that content," said Wertz. "This information helps us understand the types of indicators organizations find useful and whether we are sharing them in a timely manner."

"Capturing metadata related to which critical infrastructure sectors are sharing or acting on which indicators, for example, helps us understand how adversaries are attacking these sectors or whether there is a targeted campaign against a specific sector," Wertz continued. "We also need to improve the way we use data to feed other programs such as CDM [the Continuous Diagnostics and Mitigation program] and [the] EINSTEIN [program]."

## MODELING ADVERSARY BEHAVIORS

While AIS is important and, critically, shows how automation can shape the cybersecurity landscape, NCCIC recognizes that it must look for new ways to make attacks more difficult, time consuming, and costly for adversaries to carry out. One such strategy is the use of analytics that describe malicious behavior patterns. NCCIC shares those patterns with partners, who then look for that activity on their networks. Behavioral analytics describe actions an adversary takes while operating within a network (e.g., lateral movement, exfiltration, and credential access). This analysis helps NCCIC understand adversary tradecraft, discover security gaps, and communicate defense actions.

"At a basic level, we want to characterize adversary behavior—tactics, techniques, and procedures—in a standard, machine-readable format," said Wertz. "We then share this in the form of an analytic to customers so they can run it in their network to look for a match. This enables customers to keep data within their own infrastructure—there is no need to bring data back to DHS for analysis and correlation. Just tell us if it helped."

"Customers can look at their current defense coverage against those behaviors, assess gaps or observed behavior in their network, and act to take away the behaviors, thus significantly raising adversary costs," Wertz added. "In the federal environment, this also enables departments and agencies to identify adversary behavior and use CDM to acquire the tools and services they need to block and disrupt that behavior."

While many organizations already leverage big data analytics, NCCIC's unique position allows it to serve as a collection point for high-quality data from diverse sources. NCCIC combines data collected from federal network sensors—and shared through programs like AIS and CISC—with data from the intelligence and law enforcement communities. This set of data is growing and becoming available as departments and agencies adopt CDM.

## INCREASING DECISION SPEED THROUGH ORCHESTRATION

NCCIC is also working closely with various organizations to improve interoperability and automated cross-platform functionality within a network's defense environment. Specifically, DHS, NSA, and the John's Hopkins University's Applied Physics Laboratory developed the Integrated Adaptive Cyber Defense (IACD) framework, which helps to automate orchestration of cybersecurity products.

Often, cyber defense tools and products made by different vendors do not communicate directly with each other, meaning that cybersecurity analysts must take information from one product and manually make changes to another. This process is slow, and not an optimal use of human resources. IACD defines a framework focused on automating information sharing, risk decisions, and action. People set the rules and approve decisions or exceptions, but are otherwise not part of the operational decision loop. This frees analysts to tackle anomalies and problems that are more serious. IACD operates under the principle that effective cyber threat mitigation requires integration, synchronization, and rapid automation of capabilities across network defense layers. NCCIC can

## Leading Federal Cyber Information Sharing Efforts

The Cybersecurity Information Sharing Act of 2015 states that NCCIC should operate the Federal Government's capability and process for receiving cyber threat indicators and defensive measures.

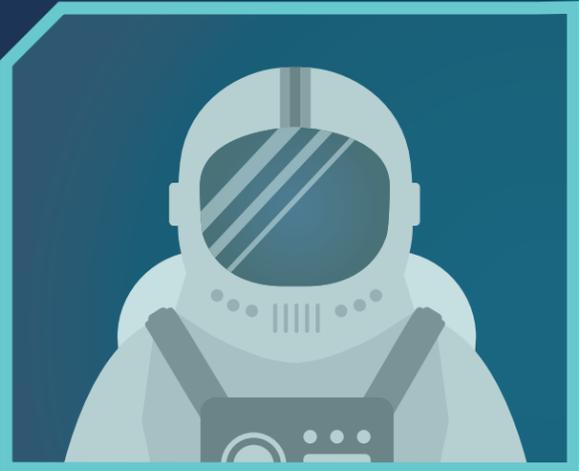
Non-federal entities that share such information through NCCIC are eligible for protections that include liability protection, protection from release under FOIA, and protection from most regulatory uses of the information.

AIS is one of the principal mechanisms through which NCCIC implements this capability and process for the Federal Government.

apply IACD concepts to the federal environment—working with agencies on behavioral analytics to identify potential gaps in coverage or vulnerabilities before exploitation—using consistent, automated workflows and processes across multiple agencies.

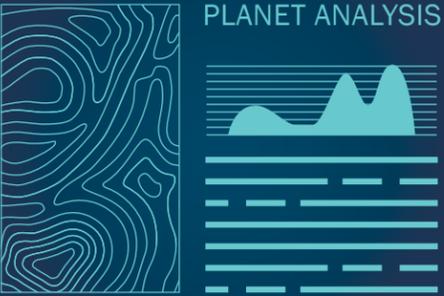
In late 2017, the Financial Services Information Sharing and Analysis Center (FS-ISAC) became the latest private sector organization to embrace IACD concepts and technologies. The use of automated workflows and orchestrations helped reduce investigation and response time from 11 hours to 10 minutes, and enabled an operations team handling 65 events per day to automatically process up to 95 events simultaneously. IACD will enable a variety of organizations to quickly share threat information and prevent and respond to cyber attacks.

Moving forward, the combination of enriched IOCs, behavioral analytics, and highly automated sharing and orchestration will be critical elements in NCCIC's cybersecurity strategy. As both the threat environment and cybersecurity technologies continue to evolve, NCCIC remains committed to finding new and better ways to work with its partners and provide them with solutions to the Nation's most intractable cybersecurity challenges.



SATELLITE UPLINK:  
MESSAGE RECEIVING

COMMANDER  
FELKER

PLANET ANALYSIS

MISSION OBJECTIVES

- PROTECT FEDERAL AND CIVILIAN AGENCIES IN CYBERSPACE
- DEFEND CRITICAL INFRASTRUCTURE
- PARTNER WITH STATE AND LOCAL GOVERNMENTS
- FORGE INTERNATIONAL PARTNERSHIPS

SCANNING FOR THREATS...

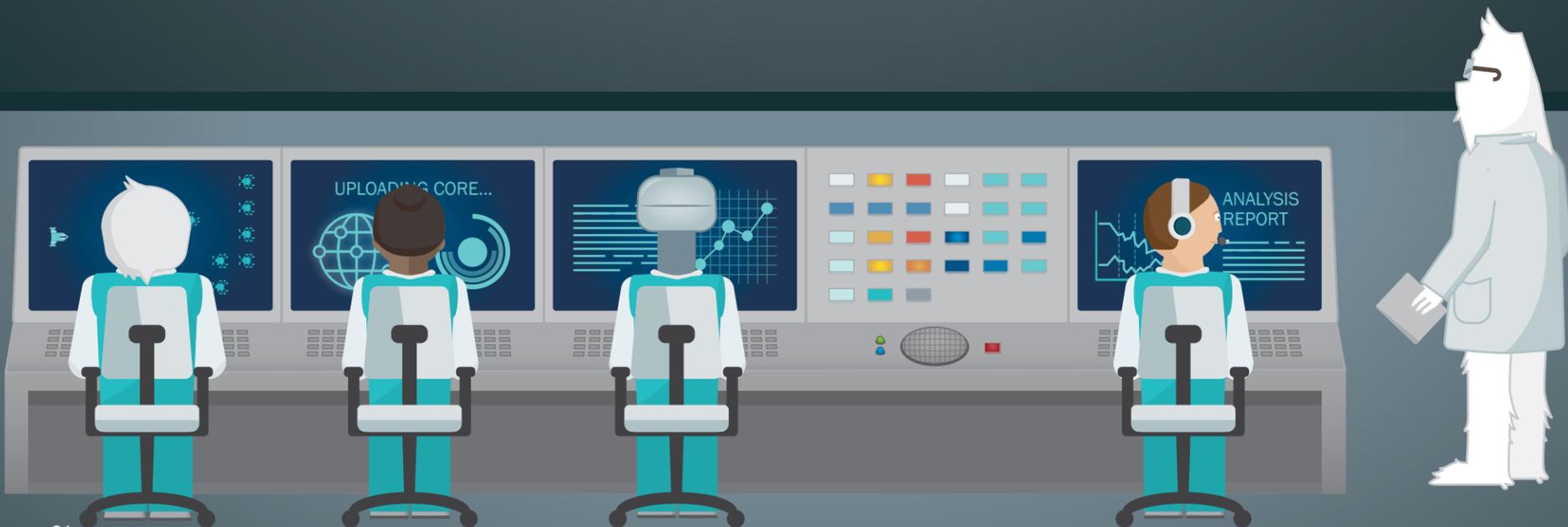
ADVANCED

MALWARE

PHISHING

# EVOLVING TO SERVE CUSTOMERS BETTER: FY 2018 AND BEYOND

In FY18, NCCIC will continue and launch a number of new initiatives to enhance services for customers, build our capabilities, and improve the efficiency and agility of our organization.



#### Developing our workforce:

NCCIC's most important asset is its people. We are making concerted efforts to retain and recruit the very best and brightest. Specifically, we are focusing on expanding our workforce to meet expected demand for incident response, risk assessment, cyber hunt services, and organizational management.

“As a highly connected nation, the United States is especially dependent on a globally secure and resilient internet and must work with allies and other partners toward maintaining...international cybersecurity priorities, including those concerning investigation, attribution, cyber threat information sharing, response, capacity building, and cooperation.”

—President Trump's Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (2017)

#### Expanding exercises and training:

To attract, retain, and maintain a technically skilled and dedicated workforce, NCCIC is offering employees opportunities to hone their expertise. Our training and exercise functions will provide internal training opportunities to our personnel—beginning with Incident Response and Assessment Qualifications as a core offering. We are also developing additional training and exercise offerings for our customers. Significant planned initiatives include additional advanced Industrial Control System (ICS) training courses and the planning and conduct of Cyber Storm VI, scheduled for Spring 2018.

#### Supporting Election Infrastructure:

NCCIC is preparing for additional requirements stemming from the FY17 establishment of Election Infrastructure (EI) as a critical infrastructure subsector of the Government Facilities Sector. In response, DHS stood up an EI Task Force, of which NCCIC is a key member. NCCIC will expand the scale and number of vulnerability scans, cyber hunt activity, and risk assessments we already conduct on our EI.

#### Realigning operations to serve customers better:

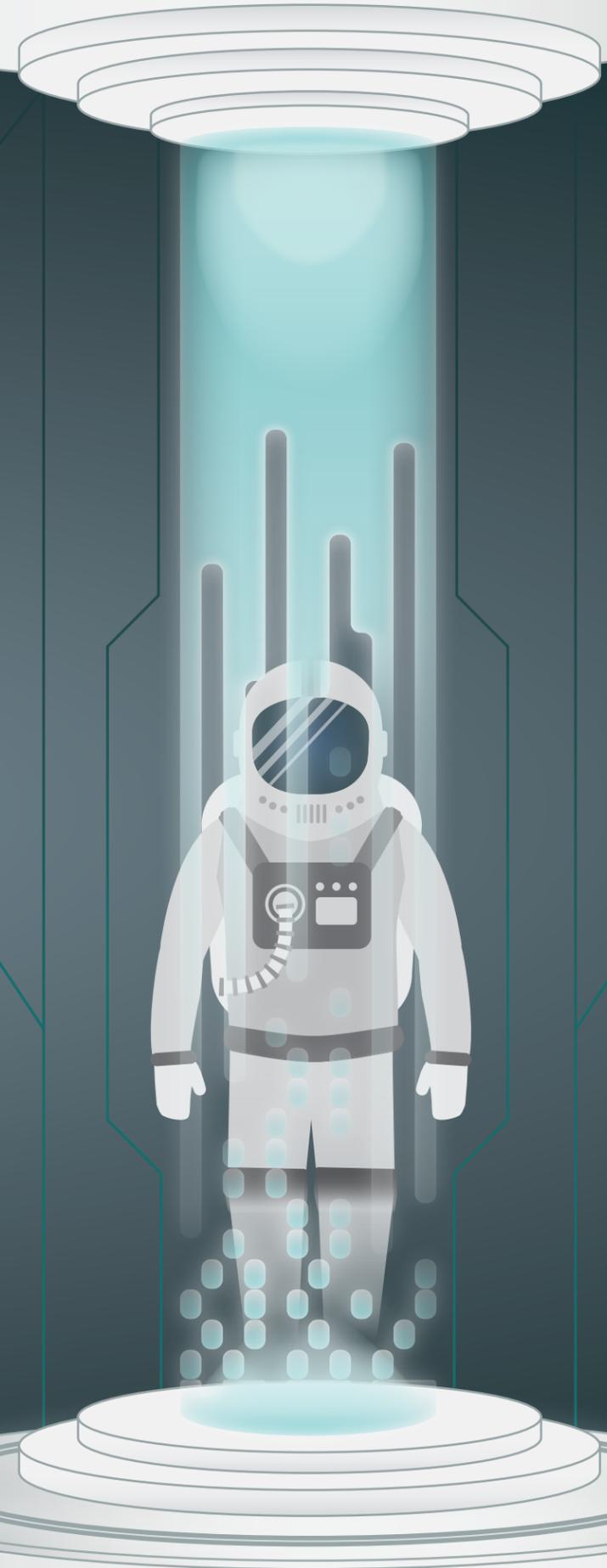
NCCIC continues to evolve the way it aligns and applies organizational resources to meet customer needs. In FY17, we combined or realigned several core functions—notably our assessment, analysis, training, operational coordination, and outreach and communications functions. These changes allow us to quickly access a larger resource pool, cross-train personnel, and streamline management and administration functions. Importantly, we continue to build our specialized technical expertise and expand partnerships to support the security of the Nation's IT, OT, and telecommunications systems. We expect these changes to translate into meaningful improvements to the way we serve and interact with our customers, partners, and other stakeholders.

#### Expanding incident response capacity:

NCCIC continues to evolve and expand its incident response capabilities to meet customer demand, as well as the requirements of Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (2017), the National Cybersecurity Protection Act of 2014, the Cybersecurity Act of 2015, and Presidential Policy Directive 41 (2016). As part of this effort, we are building toward the capability to field 12 incident response teams simultaneously, expanding our ability to provide analysis and on-site incident response to customers.

#### Enriching data and automating cybersecurity:

Throughout 2018 and 2019, NCCIC expects to enhance AIS significantly, adding context and correlation to enrich indicators of compromise (IOC) data. We will also augment our technical capabilities to better leverage behavioral analytics and automated orchestration, enabling quicker, more effective information sharing.



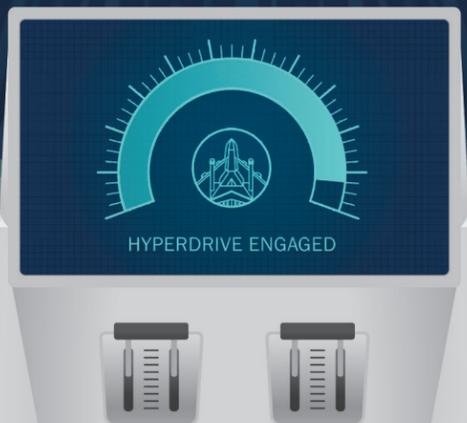
# CONCLUSION

**The risk to the Nation's cyber and communications infrastructure continues to evolve.**

In the face of increasingly sophisticated threats, NCCIC stands on the front lines of the Federal Government's efforts to defend the Nation's most essential cyber and communications networks. Every day brings challenges and opportunities. Our work inspires us, and we pursue it with a single-minded purpose: create a more secure and resilient cyber and communications infrastructure.

In pursuit of this goal, NCCIC will listen to customers, operational partners, and other stakeholders, remaining attentive and responsive to their needs. We need and will encourage active stakeholder participation

in our information sharing programs to limit the likelihood and severity of incidents. We will emphasize utility, speed, and accuracy in the information we provide, and we will share as broadly as possible, while protecting confidentiality and privacy. We will continuously assess and optimize the way we perform as an integrated organization across all locations and refine our processes, technologies, and organizational structure to best execute our mission and serve our customers. NCCIC will remain a leader in the cybersecurity field by recruiting the best and brightest people, and by remaining agile and leaning forward to tackle current and future threats.



# APPENDIX A: NCCIC SERVICES

NCCIC offers a broad portfolio of products, services, and partnership and collaboration opportunities. The offerings listed below are available without fee to NCCIC stakeholders.

For more information on NCCIC services, contact +1 (888) 282-0870 or [ncciccustomerservice@hq.dhs.gov](mailto:ncciccustomerservice@hq.dhs.gov). For more information on DHS cyber programs, visit [www.dhs.gov/cyber](http://www.dhs.gov/cyber).

## INFORMATION EXCHANGE

**Automated Indicator Sharing (AIS):** AIS is a machine-to-machine capability that receives, processes, and disseminates cyber threat indicators in real-time with the goal of reducing the number of cyber attacks.

**Cyber Information Sharing and Collaboration Program (CISCP):** CISCP is a voluntary information sharing program among critical infrastructure partners and the Federal Government. The program builds a community of trust and enhances collaboration between participants.

**NCCIC Portal:** NCCIC manages a web-based platform that allows stakeholders to securely communicate, collaborate, and share cybersecurity information and TLP:GREEN and TLP:AMBER products within trusted communities of interest.

**Website Resources:** A variety of technical and non-technical TLP: WHITE products are available on the [www.us-cert.gov](http://www.us-cert.gov) and [ics-cert.us-cert.gov](http://ics-cert.us-cert.gov) websites. Users can also subscribe to receive email notifications as products become available.

## CYBERSECURITY ASSESSMENTS

NCCIC offers a variety of assessments to help stakeholders proactively identify operational risks and measure their current security posture. These include Risk and Vulnerability Assessments, the Cyber Hygiene Program, Phishing Campaign Assessments, Red Team Assessments, and a downloadable Cyber Security Evaluation Tool (CSET).

Validated Architecture Design Reviews are conducted on Information Technology and Operation Technology. A team of experts evaluate the architecture, network traffic, and system logs—consulting with ICS subject matter experts as necessary.

Stakeholders receive recommendation and mitigation plans for all assessments.

## INCIDENT RESPONSE

NCCIC offers remote and on-site incident response capabilities, including expert intrusion analysis and mitigation guidance to customers who lack an in-house capability or require external assistance to manage a cyber incident. Technical services include network traffic analysis, host analysis, log analysis, and malware analysis.

The National Coordinating Center for Communications (NCC) coordinates 24/7 interagency and industry efforts to protect and restore communications during times of crisis.

## CYBERSECURITY TRAINING & EXERCISES

**Industrial Control Systems Training:** Classroom and online training in industrial control systems security fundamentals is available for a range of learners. Regional courses and workshops are offered, including a five-day, hands-on training event in Idaho Falls, Idaho.

**Cyber Exercises:** NCCIC supports continued improvement in national cyber preparedness and resilience through cyber exercise design, development, and conduct. Cyber Planning Workshops are offered to assist stakeholders with cyber incident response plan development.

## PUBLIC-PRIVATE PARTNERSHIPS

**Industrial Controls Systems Joint Working Group (ICSJWG):** CSJWG supports information sharing and reduced risk to the nation's industrial control systems through enhanced collaboration between the Federal Government and private owners and operators of industrial control systems across all critical infrastructure sectors.

**Communications Information Sharing and Analysis Center (ISAC):** The National Coordinating Center for Communications (NCC) serves as the operational arm of the Communications Information Sharing and Analysis Center (Comm-ISAC) and facilitates the exchange of vulnerability, threat, and intrusion information.

**CISCP Advanced Technical and Training Exchange (ATTE):** NCCIC hosts quarterly, day-long meetings for network defenders within the CISCP community to collaborate and discuss cyber threat trends, activity, and cybersecurity best practices.

## FEDERAL NETWORK PROTECTION

**EINSTEIN:** NCCIC operates and manages the EINSTEIN program, which consists of systems to detect and prevent intrusions. EINSTEIN provides automated processes for collecting, correlating, analyzing, and sharing computer security information across the Federal Government to improve our Nation's cybersecurity posture.

## MALWARE ANALYSIS AND VULNERABILITY COORDINATION

**Advanced Malware Analysis Center:** The Advanced Malware Analysis Center provides 24/7 dynamic analysis of malicious code. Samples may be submitted online using the "Report Malware" option on [www.us-cert.gov](http://www.us-cert.gov).

**Advanced Analytical Laboratory (AAL):** The AAL, located at Idaho National Laboratory, analyzes malware threats to control system environments and provides asset owners with onsite or remote support.

**Vulnerability Coordination:** NCCIC works with trusted partners in the public and private sectors to coordinate timely and responsible disclosure of vulnerabilities. Risks are publicized only after practical and effective mitigations are available to users and administrators.

## INTERAGENCY COORDINATION

**Joint Agency Cyber Knowledge Exchange (JACKE):** NCCIC hosts a quarterly discussion of current threats and response strategies for cybersecurity professionals.

**Security Operations Center (SOC) Coordination:** NCCIC coordinates a weekly teleconference for SOC analysts to discuss tactical-level trends observed.

**Federal Cybersecurity Interagency Group (FCIG):** NCCIC organizes a monthly meeting for cybersecurity centers to collaborate on a variety of cybersecurity issues. Discussion topics include cybersecurity policy, operations, and technology use.



**IN THE BATTLE FOR  
CYBERSPACE,  
YOU ARE  
NOT ALONE**

---

NCCIC YEAR IN REVIEW 2017  
OPERATION CYBER GUARDIAN



Homeland  
Security

NATIONAL CYBERSECURITY  
AND COMMUNICATIONS  
INTEGRATION CENTER