Resources and Capabilities Guide

The National Cybersecurity and Communications Integration Center (NCCIC)

October 21, 2013

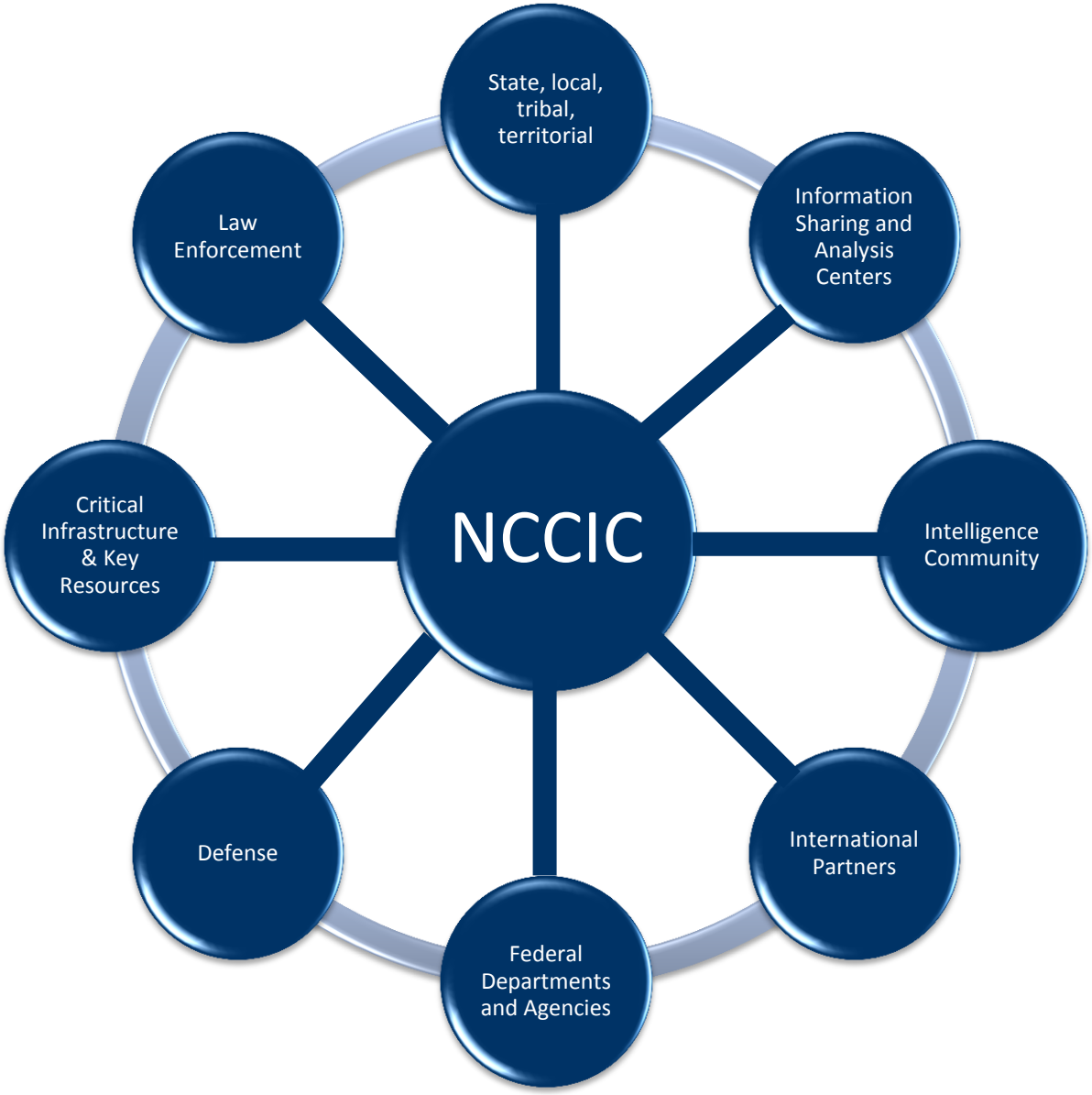
Homeland Security

National Cybersecurity and Communications Integration Center

Contents

I. Purpose

The National Cybersecurity and Communications Integration Center (NCCIC) Resource and Capabilities Guide is intended to enhance cross-sector cyber security efforts and collaboration by better informing our cybersecurity and communications partners of the NCCIC's tools, assets, and collaboration mechanisms offered. This guide also identifies the Center's resources and capabilities as well as describes the processes for accessing NCCIC information portals and products, incident reporting systems, and relevant point of contact information for our community of partners.



II. Introduction

The Department of Homeland Security (DHS) is responsible for protecting the Nation's critical infrastructure from physical and cyber threats. Cyberspace has united once distinct information structures, including business and government operations, emergency preparedness communications, and critical digital and process control systems and infrastructures. Protection of these systems is essential to the resilience and reliability of the Nation's critical infrastructure and key resources (CIKR) affecting economic and national security.

NCCIC Overview

The National Cybersecurity & Communications Integration Center (NCCIC), within the Office of Cybersecurity and Communications (CS&C) (http://www.dhs.gov/office-cybersecurity-and-communications), serves as a centralized location where operational elements are coordinated and integrated. NCCIC partners include all federal departments and agencies; state, local, tribal, and territorial (SLTT) governments; the private sector; and international entities. The NCCIC's activities include providing greater understanding of cybersecurity and communications situation awareness vulnerabilities, intrusions, incidents, mitigation, and recovery actions.

NCCIC Vision

A world class cybersecurity and communications organization performing cutting edge analysis, sharing actionable and comprehensive information in real time, and ensuring a whole-of-nation approach to response, mitigation, and recovery efforts.

NCCIC Mission

To operate at the intersection of the private sector, civilian, law enforcement, intelligence, and defense communities, applying unique analytic perspectives, ensuring shared situational awareness, and orchestrating synchronized response efforts while protecting the Constitutional and privacy rights of Americans in both the cybersecurity and communications domains.

The NCCIC's missions include:

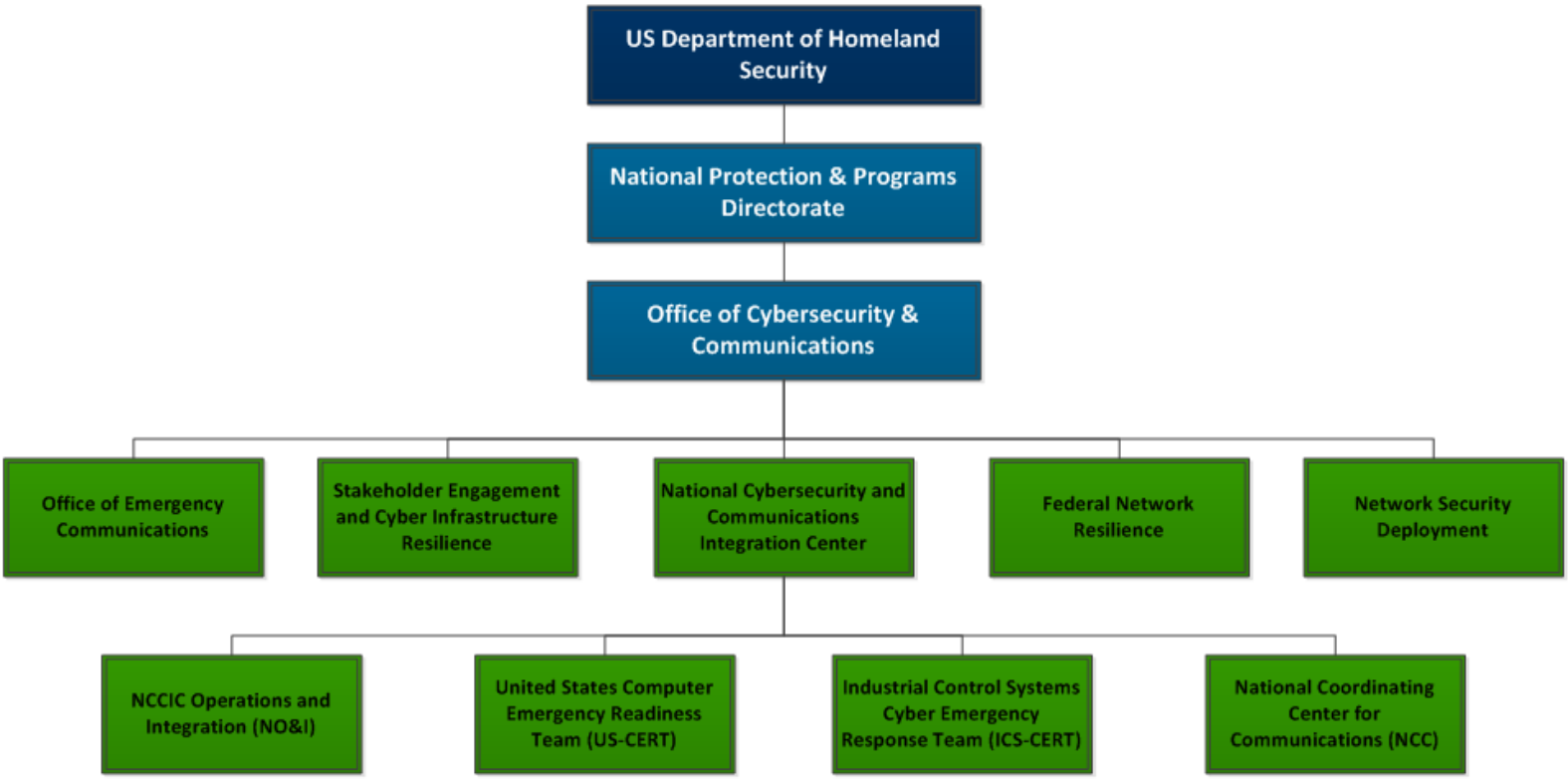
- Protection of federal civilian agencies in cyberspace;
- Working closely together with critical infrastructure owners/operators and sector specific agencies to reduce risk;
- Collaborating with state and local governments through the Multi-State Information Sharing and Analysis Center (MS-ISAC);
- Cooperating with international partners to share information and respond to incidents;
- Coordinating national response to significant cyber incidents in accordance with the National Cyber Incident Response Plan (NCIRP);
- Analyzing data to develop and share actionable mitigation recommendations;
- Creating and maintaining shared situational awareness among its partners and constituents;

- Orchestrating national protection, prevention, mitigation, and recovery activities associated with significant cyber and communication incidents;
- Disseminating cyber threat and vulnerability analysis information; and
- Assisting in the initiation, coordination, restoration, and reconstitution of National Security or Emergency Preparedness (NS/EP) telecommunications services and facilities under all conditions, crises, or emergencies, including executing Emergency Support Function 2- Communications (ESF-2) responsibilities under the National Response Framework (NRF).

The NCCIC is comprised of four branches:

- NCCIC Operations & Integration (NO&I);
- United States Computer Emergency Readiness Team (US-CERT);
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT); and
- National Coordinating Center (NCC) for Communications.

As mutually supporting, fully integrated elements of the NCCIC, these branches provide capabilities and partnerships necessary to lead a whole-of-nation approach to addressing cybersecurity and communications issues at the operational level.



NO&I develops operational planning, training, and exercises for the NCCIC. Managing a portfolio of cyber exercises ranging from small-scale, discussion-based exercises to large-scale, operations-based exercises such as DHS's flagship Cyber Storm Exercise Series (http://www.dhs.gov/cyber-storm-securing-cyber-space), NO&I also participates in the planning and execution of national, international, SLTT, and private sector exercises.

US-CERT brings advanced network and digital media analysis expertise to bear on malicious activity targeting the Nation's networks. US-CERT develops timely and actionable information for distribution to federal departments and agencies, SLTT governments, private sector organizations, and international partners. In addition, US-CERT operates the National Cybersecurity Protection System (NCPS), which provides intrusion detection and prevention capabilities to covered federal departments and agencies.

ICS-CERT reduces risk to the Nation's critical infrastructure by strengthening control systems security through public-private partnerships. ICS-CERT has four focus areas: situational awareness for CIKR stakeholders; control systems incident response and technical analysis; control systems vulnerability coordination; and strengthening cybersecurity partnerships with government departments and agencies.

NCC leads and coordinates the initiation, restoration, and reconstitution of NS/EP telecommunications services or facilities under all conditions. NCC leverages partnerships with government, industry and international partners to obtain situational awareness and determine priorities for protection and response.

The NCCIC also relies heavily on voluntary collaboration with its partners. The NCCIC works closely with those federal departments and agencies most responsible for securing the government's cyber and communications systems, and actively engages with private sector companies and institutions, state, local, tribal, and territorial governments, and international counterparts. Each group of stakeholders represents a community of practice, working together to protect the portions of critical information technology that they own, operate, manage, or interact with.

III. Information Sharing

The NCCIC's information sharing avenues include websites, portals, written reports, and meetings which are available to provide accurate and actionable threat and tactical information. The NCCIC provides in-person information sharing programs to enhance knowledge and collaboration among public and private sector partners. NCCIC training and exercise programs also improve threat awareness, detection, and readiness capabilities. In addition, the NCCIC holds an NCCIC Monthly Analysis Meeting on NCCIC products – a meeting that is open to all partners. This meeting provides an opportunity for open communication between the NCCIC and its outside affiliates. If you are interested in attending, please e-mail NCCIC@hq.dhs.gov .

Report Types

The NCCIC produces several reports to alert partners of emerging cyber threats, vulnerabilities, and current activities. Certain products such as Alerts, Current Activity, Bulletins, and Tips are released through US-CERT's National Cyber Awareness System (NCAS). To sign up for NCAS products, visit their Subscription System and Mailing Lists and Feeds (http://www.us-cert.gov/ncas) page. The remaining products are distributed by other means, which are described later in the document. The following is the full list of NCCIC products:

Advisories - Provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks. Advisories describe the affected products and the impact it had the system or network, the vulnerabilities and mitigation.

Alert & Situation Reports - Alerts serve as the vehicle for expedited notification of key stakeholders when an event meets an NCCIC Principal Information Requirement. As events develop and more information becomes available, Alerts may be updated with periodical "Situation Reports" (or SITREPs) which prominently feature the most up-to-date details and projections on the topic of the original Alert.

Analysis Reports - Analytic products that provide analysis and insight into specific tactics, techniques and procedures (TTPs) describing the activity, how to detect it, defensive measures and remediation advice, as appropriate. Analysis Reports typically contain the attack string, the IP address and domains affected and other pertinent information related to the attack.

Current Activity Updates - Current Activity Updates will provide information of an event involving a vulnerability, threat, or imminent or ongoing attacks. Updates may describe high level descriptions of new system or software releases or vulnerabilities in a system or network and potential impacts and mitigation.

Daily Summaries - Daily Summaries will provide our partners with recent activities which have been detected or reported and the steps necessary to mitigate the threats. Summaries may contains current news and events, reported incidents, ports/protocol activities, and new vulnerabilities and threats.

Indicator Bulletins - Indicator Bulletins are intended to provide incident analysis and timely information derived from new cyber incidents and/or malicious code, threats, and vulnerabilities. The intended audience for these products may include federal, state, or local governments, critical infrastructure private industry partners, and national CERTs.

Periodic Newsletters - Periodic Newsletters provide information to partners regarding malicious activity, situational awareness, training updates, assessment summaries, recent product releases, open source situational awareness highlights, upcoming events, and coordinated vulnerability disclosures.

Recommended Practices - Recommended Practices provide guidance on the tools and techniques users should apply to their public facing websites, network, and/or host computers in order to increase security.

Weekly Analytic Synopsis Product (WASP) – The WASP provides a general overview of trending cyber threats and the increase or decrease in incident reports for known threats. The contents include a summary of incident response within the federal government, specific cyber threats such as malware, phishing, and botnets, and other emerging threats as well as tactical indicators for use in computer network defense. In addition, the NCCIC offers the *Cyber Snapshot*, which has the same framework as a WASP but may include sensitive and/or classified material. To receive the WASP or Cyber Snapshot, please contact NCCIC@hq.dhs.gov. For the classified report, the individual must have a Joint Worldwide Intelligence Communication System (JWICS) e-mail and send their full name, agency/company name, and the last four digits of their social security number to the e-mail referenced above. NCCIC Watch and Warning will then send the applicant's information for clearance validation to ensure they have all compartments at the Sensitive Compartmented Information (SCI) level.

Weekly Digests - Provide documented and categorized cybersecurity incidents, such as malicious activity, encountered throughout the civilian federal government. Weekly Digests also contain a list of attacking domain/IP addresses and indicators which must remain in U.S. government channels or other designated channels outlined in non-disclosure agreements.

Year in Review - The Year in Review provides information to a global audience involving accomplishments, analysis of activity, and publications disseminated within a given year.

Information Sharing Programs

The NCCIC and its DHS partners maintain a number of integrated information sharing initiatives to rapidly share information about current cyber activity. CS&C's Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR) division acts as the primary point of engagement and coordination for NS/EP communications and cybersecurity initiatives. Through these programs, the NCCIC seeks to develop trusted communities among public and private sector entities, enhance collaboration, and build threat knowledge. The following sections describe information sharing programs and capabilities.

Cyber Information Sharing and Collaboration Program (CISCP)

The CISCP supports improvements to the defensive posture of CIKR entities by facilitating the exchange of current threats and vulnerabilities affecting both critical infrastructure and government sources. The goal of the program is to create an effective information sharing framework among the government, Information Sharing and Analysis Centers and related organizations, information and communications technology service providers, and their respective critical infrastructure owner/operator members and customers.

CISCP participants sign a Cooperative Research and Development Agreement (CRADA), which is the main governance vehicle in this program, which also provides the opportunity for physical presence on the NCCIC watch floor. Key benefits of using a CRADA include enabling bi-directional data flow that protects both entity enterprise networks and customers, ensuring access to all CISCP data, and enabling analytical collaboration.

For further information, please email ciscp_coordination@hq.dhs.gov.

Enhanced Cybersecurity Services (ECS)

ECS is a voluntary information sharing program that assists critical infrastructure (CI) owners and operators to improve protection of their systems from unauthorized access, exploitation, and data exfiltration. ECS protects CI entities, develops threat "indicators," and has the ability to share these sensitive and classified cyber threat indicators with qualified Commercial Services Providers (CSPs).

ECS services are intended to augment, not replace, existing cybersecurity services operated by or available to CI entities. It is important to note that protection of privacy, government intelligence, and corporation information is paramount to this voluntary program. SLTT governments and validated CI entities from all CI sectors are eligible to participate in the ECS program.

CSPs are also critical to enhancing cyber defense in the Nation's critical infrastructure and a vital component to the ECS program. In order to participate in the program, CPSs must meet eligibility requirements, vetting criteria, and sign a Memorandum of Agreement (MOA) with DHS. CSPs are also responsible for handling, using, and maintaining all sensitive and classified information in accordance with defined security requirements.

For more information please visit, http://www.dhs.gov/enhanced-cybersecurity-services.

Web-based Platform Access

The NCCIC provides many web-based information sharing compartments within the US-CERT Portal to facilitate collaboration. Each compartment has unique content for specific NCCIC partners and entities. The following sections indicate what each compartment contains and how to gain access.

Portal Access

The NCCIC provides a secure, web-based, collaborative system to share sensitive, cyber-related information and news with partners. The recommended compartments for information sharing are the Cobalt and Control System (CS) Compartments, which hold information regarding cyber indicators, incidents, and malware digests for critical infrastructure systems. The Cobalt Compartment serves as an information hub for enterprise systems security, while the CS Compartment provides material on industrial control systems and is limited to control system asset owners/operators. An individual or organization can request access to the Cobalt Compartment by sending an e-mail to NCCIC_Partnership@hq.dhs.gov with the subject line as, "Request access to Cobalt Compartment". To access the CS Compartment, send an e-mail to NCCIC_Partnership@hq.dhs.gov with the subject line as, "Request access to Control Systems Compartment."

In order to qualify for either compartment, requestors must:

- Be a U.S.- based organization;
- Have professionals working in a network defense or cybersecurity incident response role within an organization; and
- Be members of international federal cyber incident response teams or non-governmental computer network defense organizations.

National Coordinating Center (NCC) for Communications Information Access

To receive information from the NCC, please e-mail NCCIC@hq.dhs.gov and ask to be added to the NCC distribution list. The NCCIC will review and grant access based upon authorization by the NCC approval authority.

NCCIC Websites

The National Cybersecurity and Communications Integration Center
- http://www.dhs.gov/about-national-cybersecurity-communications-integration-center

The United States Computer Emergency Readiness Team
- http://www.us-cert.gov/

The Industrial Control Systems Cyber Emergency Response Team
- http://ics-cert.us-cert.gov/

National Coordinating Center for Communications
- http://www.dhs.gov/national-coordinating-center-telecommunications

IV. Technical Assistance, Analysis, and Reporting

The NCCIC, through its internal components and partners, coordinates situational awareness and cyber incident mitigation for current and potential security threats to partners. This section describes the three operational components, the NCCIC's assessment and technical services, and incident reporting.

United States Computer Emergency Readiness Team (US-CERT)

The NCCIC's United States Computer Emergency Readiness Team (US-CERT), within the Department of Homeland Security's (DHS) Office of Cybersecurity and Communications (CS&C), was created in September 2003 to help protect the Nation's Internet infrastructure by coordinating defense against and response to cyber-attacks. US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities. As a trusted global leader in cybersecurity, US-CERT builds and leverages partnerships to gain knowledge and raise awareness around the clock.

US-CERT has multiple proficiencies to further NCCIC's vision and mission:

- Subject Matter Experts in IT Network Architectures
    - Networking technologies, malware, digital forensics, enterprise network solutions

- State of the Art Advanced Malware Analysis Center (AMAC)
    - The AMAC provides US-CERT with the capability to collect, analyze, and exchange up-to-date malware information 24 hours a day. Elements of its operation are: conducting advanced automated analysis of malware samples; correlating common characteristics across millions of malicious code artifacts; and investigating malware in a safe, secure, and contained environment.
    - As of August 27, 2013, AMAC's Artifact Catalog contains 60,260,134 artifacts. Not all artifacts are malware samples, some of them contain links to known sites where malware is present or has been present.

- Network, System and Host Analysis on Enterprise Systems
    - Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS) Logs
    - Proxy and Network Infrastructure Logs
    - Network Traffic Analysis
    - Disk and Firmware Images

- Support for Incident Response, Recovery and Future Defense Efforts

National Cybersecurity Assessment & Technical Services (NCATS)

The NCATS supports the NCCIC's mission by leveraging existing "best in breed" cybersecurity assessment methodologies, commercial best practices and integration of threat intelligence that enables cybersecurity stakeholders with decision making/risk management guidance and recommendations.

NCATS provides an objective third-party perspective on the current cybersecurity posture of the stakeholder's unclassified operational/business networks.

NCATS security services are available at no-cost to stakeholders and can range from one day to two weeks depending on the security services required. Security services currently available are:

- Network Scanning
- Vulnerability Scanning and Testing
- Penetration Testing
- Social Engineering (Phishing)
- Web Application Scanning and Testing
- Operating System Scanning
- Database Scanning
- Mainframe Assessment
- Wireless Discovery and Identification

The NCATS team consists of subject matter experts in penetration testing methodology and tactical delivery. Team members have extensive experience in current and emerging web applications, networks, databases, wireless, mobile computing, cloud security, social engineering, social media and intelligence gathering.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

The NCCIC's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), within the Department of Homeland Security's (DHS) Office of Cybersecurity and Communications (CS&C), works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among federal, state, local, and tribal governments and control systems owners, operators, and vendors.

Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures. The following are the capabilities that ICS-CERT deploys to protect the nation's CIKR systems:

- ICS Cybersecurity Training
    - Introductory free on-line web-based training courses for Operational Security for Control Systems (OPSEC for Control Systems).

- Advanced hands-on with a Red Team/Blue Team exercise in an actual control systems environment.

- Subject Matter Experts in Industrial Control Systems (ICS)
  - Supervisory Control and Data Acquisition (SCADA), Process Control Systems (PCS), Distributed Control Systems (DCS), Remote Terminal Units (RTUs), Human Machine Interfaces (HMIs), Programmable Logic Controllers (PLCs).

- Cyber Security Evaluation Tool (CSET)
  - Consistent and repeatable methodology based upon recognized sector-specific standards
  - Free stand-alone software tool for assisting owners of networks and ICS with evaluating and strengthening their cybersecurity posture.

- Prioritized & Measurable ICS-CERT Cybersecurity Solutions
  - ICS-CERT utilizes an iterative process of tangible measurements based upon NIST 800-53 and the Cyber Security Evaluation Tool (CSET) followed by focused mitigations and gap analysis, DHS and the company can prioritize resource decisions to invest in areas that deliver the highest possible return on investment for both the government and the private sector.
  - By leveraging information supplied by Infrastructure Protection's Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), will offer prioritized access to products and services designed to be effective across the entire cybersecurity protection spectrum to those companies identified as being most critical within their given sector.

- Unique Awareness of Emerging Issues and Threats to Control Systems and Vendor Products

- State of the Art Analysis Capabilities Specific to ICS that enable the following:
  - Malware and Embedded Systems Analysis
  - Patch Testing
  - Consequence Analysis

- Onsite Consultation and Self-Evaluations
  - Helping ICS asset owners take preventative measures necessary to prepare for and protect from cyber attacks
  - No cost on-site defense-in-depth cybersecurity strategic analysis of critical infrastructure by DHS subject matter experts

- Incident Response Support for ICS-Related Response, Recovery and Future Defense Efforts

National Coordinating Center (NCC) for Communications

The National Coordinating Center (NCC) for Communications, within the Department of Homeland Security's (DHS) Office of Cybersecurity and Communications (CS&C), facilitates the exchange among government and industry participants regarding vulnerability, threat, intrusion, and anomaly information affecting the communications infrastructure. The NCC has numerous capabilities to perform its responsibilities within the NCCIC:

- Subject Matter Experts in all Communication Domains
  - Wireless (Cellular, Satellite, Microwave)
  - Wireline (Public Switched Telephone Network, Internet, Signaling Systems, Physical Infrastructure)

- Enrollment in Priority Service and Priority Restoration Programs
  - Government Emergency Communications Service (GETS)
  - Wireless Priority Service (WPS)
  - Communications Service Priority (TSP)

- Real-time Access to Telecom/Internet Service Providers During Cyber Events

- Support for Emergency Support Function # 2 (ESF-2)
  - Emergency Response Function for Events Impacting NS/EP Communications
  - Consequence Management support in Collaboration with FEMA

Reporting a Cyber or Communications Incident to the NCCIC

The NCCIC operates 24 hours a day, 7 days a week, 365 days a year, and can be reached at 1-888-282-0870 or by visiting the reporting web form shown at https://forms.us-cert.gov/report.

When to report an incident:
If there is a suspected or confirmed cyber or communications event or incident that:

- Affects core government functions;
- Affects critical infrastructure functions;
- Results in a significant loss of data, system availability, or control of systems; or
- Indicates malicious software is present on critical systems.

What to report (if known):

- Your name, organization, address, and phone number
- What organization experienced the incident?
- Who is the point of contact at the affected entity?
- Are the affected systems owned by the government or the private sector?
- What systems have been affected?

- What are the impacts?
- What was compromised or disclosed?
- Is the affected entity requesting federal assistance?
- How the incident was initially detected or discovered?
- Who else has been made aware of the incident?

US-CERT Reporting

To submit a malware sample, send the sample to the Advanced Malware Analysis Center (AMAC) at submit@malware.us-cert.gov. Customers must provide a password-protected .zip file using password "infected."

To report a phishing scheme, please visit http://www.us-cert.gov/report-phishing/and make sure to follow the methods of reporting phishing e-mails on the website to ensure security.

ICS-CERT Reporting

To report a cyber event on control systems/critical infrastructure please call 1-877-776-7585 or e-mail ICS-CERT at ics-cert@hq.dhs.gov.

To report ICS software vulnerability please visit http://www.kb.cert.org/vuls/html/report-a-vulnerability/ and fill out the Vulnerability Reporting Form. Please follow the directions to encrypt to the CERT Pretty Good Privacy (PGP) key in order to protect sensitive, non-public vulnerability information.

NCC Reporting

Please contact the NCC to report an incident if an event:

- Affects core government communications functions;
- Affects critical infrastructure communications functions; or
- Indicates malicious software is present on critical communications systems.

To contact the NCC Watch, please call 1-703-235-5080 or e-mail NCC@hq.dhs.gov. If any proprietary information is involved, please specify the extent of dissemination of that information.

Multi-State Information Sharing and Analysis Center (MS-ISAC) Reporting

State, local, tribal, or territorial government representatives who believe they are experiencing a cyber event can also report to the 24x7 MS-ISAC Security Operations Center at 1-866-787-4722, or can submit online by visiting http://msisac.cisecurity.org/about/incidents/ and clicking on the "Report an Incident" button.

United States Secret Service (USSS) Electronic Crimes Task Force Reporting (ECTF)

It is the goal of the ECTFs to combine the resources of academia; the private sector; and local, state and federal law enforcement agencies to, "prevent, detect and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems."

The ECTFs focus on several types of investigations to include: network intrusions, hacking attacks, phishing schemes, skimming, access device fraud, carding portals, wire fraud, use of malicious software and other computer-related offenses. To report any malicious activities, please visit http://www.secretservice.gov/ectf.shtml, and select an ECTF location for event reporting.

Incident Response Contacts

The following contacts are for the operational components of the NCCIC. The NCCIC will evaluate the information you provide and track the incident for appropriate follow-up based on severity.

NCCIC Contact	Phone #	Email Address
US-CERT	1-888-282-0870	NCCIC@us-cert.gov
ICS-CERT	1-877-776-7585	ICS-CERT@hq.dhs.gov
NCC	1-703-235-5080	NCC@hq.dhs.gov

NCCIC Component	Why Government/Industry would call?	What is done to help?
US-CERT	**Examples include:** -Compromise of enterprise systems -Malicious software -Data exfiltration -DDoS of mission critical systems -Complex spear phishing	-Provide mitigation and coordination -Can help provide incident response, recovery, and future defense efforts -Analyze malware malicious files, email, and hard drive images -Send out advisories and situation awareness
ICS-CERT	**Examples include:** -Compromise of industrial control systems -Malicious malware -Data exfiltration -Exploitation of vulnerabilities	
NCC	**Examples include:** -Mobile malware -Degradation/denial of communication	

V. Assessments, Training, Planning, and Exercises

The NCCIC plays an active role in the facilitation of various training and operations exercises to build the collective knowledgebase of its partners and test integrated operational processes. The following section describes the several assessments, training, planning, and exercise mechanisms at the NCCIC.

Assessments

National Cybersecurity Assessment & Technical Services (NCATS)

NCATS supports the NCCIC mission by leveraging existing "best in breed" cybersecurity assessment methodologies, commercial best practices and integrating threat intelligence that enables cybersecurity stakeholders with decision making/risk management guidance and recommendations. NCATS has branded this as the "Absolute State of the Hack" mindset and methodology.

NCATS provides an objective third-party perspective on the current cybersecurity posture of the stakeholder's unclassified operational/business networks.

For additional information on NCATS security services, scheduling, timeline and expectations please e-mail NCATS_Info@hq.dhs.gov.

Cyber Security Evaluation Tool (CSET) Assessment

The Cyber Security Evaluation Tool (CSET®) is a self-contained software tool which runs on a desktop or laptop computer. It evaluates the cybersecurity of an automated, industrial control or business system using a hybrid risk and standards-based approach, and provides relevant recommendations for improvement.

For all information regarding CSET Assessments please visit http://ics-cert.us-cert.gov/Assessments. This site will give you an overview of the assessment tool, purpose, key benefits, and how to obtain CSET.

Training

ICS-CERT Training

To view ICS-CERT training sessions please visit https://ics-cert.us-cert.gov/Calendar which shows the schedule of events that may be of interest to control systems security personnel. ICS-CERT also provides web-based training for Operational Security for Control Systems located at http://opsecics.inl.gov/dhsopsecr01/player.html.

Additional training focusing on aspects of technical security for the ICS environment can be found on the ICS-CERT website at https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT.

Texas A&M Engineering Extension Service (TEEX)

The TEEX Cybersecurity online courses are designed to ensure that the privacy, reliability, and integrity of the information systems that power our global economy remain intact and secure. These DHS/FEMA-certified courses are offered through three discipline-specific tracks targeting general, non-technical computer users, technical IT professionals, and business managers and professionals. TEEX operates comprehensive cybersecurity training program online, at http://www.teexwmdcampus.com/index.k2#. The online cybersecurity courses are designed to ensure the confidentiality; availability and integrity of the information systems that power our global economy. All online courses are designed to provide an entry-level understanding of the topics and are designed to help students prepare for Advanced Training provided by the National Emergency Response and Rescue Training Center (NERRTC) in your jurisdiction.

Federal Virtual Training Environment (FedVTE) [FED ONLY]

The FedVTE content library contains pre-recorded classroom training that users can access anytime, anywhere. Audio and video recordings are synchronized with a transcription and instructor slides. If users pause or exit, FedVTE will remember where they left off. The new FedVTE is easier to use, has new courses and labs, and supports nearly twice as many users. FedVTE is open to military and civilian users from across the U.S. federal government. Additional features include:

- 550 hours of training, 150 demos, and 3,000+ pieces of content
- Fast forward, rewind, highlight text, and add personalized notes
- View and print training certificates and progress reports

To sign up, please visit https://www.fedvte-fsi.gov/Vte.Lms.Web . If you have additional questions, contact the FedVTE help desk at FedVTE-FSIHelp@state.gov .

Planning

The NCCIC Operational Planning, Exercise, Training, and Integration Unit (OPETIU) supports the development, organization, and execution of cyber and communication incident response capabilities across a wide spectrum of potential threats and targets. OPETIU works with federal, state, and sector stakeholders to develop operational planning products.

Key operational planning products include:

- NCCIC Operational Planning Approach
- Energizer Incident Action Plan
- Sector Specific Operations Playbooks

Exercises

Cyber Storm Exercise Series

The Cyber Storm (CS) exercise series supports the preparedness and response goals established in the National Strategy to Secure Cyberspace as well as Homeland Security Presidential Directive 8 (HSPD-8) and is the Department's flagship national-level cyber exercise.

DHS hosted CS I in 2006, CS II in 2008, and CS III in 2010. Beginning in November 2011 and continuing through 2013, CS IV consists of multiple, targeted building block exercises and involves over 1000 worldwide participants representing six Cabinet-level departments, 17 states, 11 international partners, and more than 30 private sector companies and coordination bodies.

For more information on cyber exercises, contact OPETIU at CEP@hq.dhs.gov.

National and International Exercises

Operational Planning, Exercise, and Training Integration Unit (OPETIU) participates in the planning and execution of intra- and inter-agency national-level exercises and provides cyber exercise assistance to federal partners when needed. This planning includes coordination with the Federal Emergency Management Agency's exercise initiatives, the National Level Exercise (NLE) series, and other federal exercises, as appropriate. OPETIU was a major contributor to NLE 2012 which highlighted challenges in detecting, assessing, and responding to a significant cyber event.

Because cyber threats do not adhere to political or geographical boundaries, OPETIU encourages improved international cybersecurity cooperation through bilateral and multi-lateral efforts. Through various DHS international operational and policy initiatives, OPETIU sponsors tabletop exercises and workshops to raise awareness and advance global cybersecurity coordination strategies.

State, Local, Tribal, and Territorial Exercises

OPETIU directly supports state, local, tribal, and territorial (SLTT) cyber exercise design, development, and conduct. OPETIU's cyber exercises familiarize SLTT cyber and all-hazards stakeholders with the roles, responsibilities, policies, plans and procedures related to cyber incidents. In response to SLTT requests, OPETIU provides the cyber exercise direct support as a free service.

Sector Exercises

In support of the private sector, OPETIU has developed an adaptable and scalable Cyber Tabletop Exercise Package (CTEP) for, and with, the following sectors: Chemical, Commercial Facilities, Critical Manufacturing, and Healthcare and Public Health.

This free package allows private sector planners to produce a high-quality, discussion-based cyber exercise that suits their needs. OPETIU is currently in the process of expanding this CTEP offering.

VI. Conclusion

The NCCIC resource guide aims to be a helpful document to highlight the various capabilities and offerings that the NCCIC has to offer partners for steady state and cyber incident management needs. Please reach out to at any time if you have any questions, concerns, or recommendations. The following appendices further highlight and describe the programs we have noted in this document for additional clarity.

Can I share this product?

Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

APPENDIX A: NCCIC SUMMARY

Homeland Security

National Cybersecurity and Communications Integration Center

NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

The U.S. Department of Homeland Security (DHS) is responsible for protecting our Nation's critical infrastructure from physical and cyber threats. This vital mission requires effective coordination and collaboration among a broad spectrum of government and private sector organizations. To better manage and facilitate U.S. cybersecurity efforts, DHS established round-the-clock operations coordinating center, the National Cybersecurity and Communications Integration Center (NCCIC) within its Office of Cybersecurity and Communications (CS&C).

Cyberspace enables businesses and government to operate, facilitates emergency preparedness communications, and enables critical control systems processes. Protecting these systems is essential to the resilience and reliability of the Nation's critical infrastructure and key resources and to our economic and national security.

The NCCIC's mission is to operate at the intersection of the private sector, civilian, law enforcement, intelligence, and defense communities, applying unique analytic perspectives, ensuring shared situational awareness, and orchestrating synchronized response efforts while protecting the Constitutional and privacy rights of Americans in both the cybersecurity and communications domains.

NCCIC RESPONSIBILITIES

The NCCIC's role is to lead the protection of federal civilian agencies in cyberspace, provide support and expertise to critical infrastructure owners and operators, work through the Multi-State Information Sharing and Analysis Center (MS-ISAC)to provide expertise and information to state and local governments, and coordinate with international partners to share information and collaboratively respond to incidents.

The NCCIC's responsibilities include:

- Leading the protection of federal civilian agencies in cyberspace;
- Working closely together with critical infrastructure owners and operators to reduce risk;
- Collaborating with state and local governments through the Multi-State Information Sharing and Analysis Center (MS-ISAC);
- Cooperating with international partners to share information and respond to incidents;
- Coordinating national response to significant cyber incidents in accordance with the National Cyber Incident Response Plan (NCIRP);
- Analyzing data to develop and share actionable mitigation recommendations
- Creating and maintaining shared situational awareness among its partners and constituents;
- Orchestrating national protection, prevention, mitigation, and recovery activities associated with significant cyber and communication incidents;
- Disseminating cyber threat and vulnerability analysis information;
- Assisting in the initiation, coordination, restoration, and reconstitution of National Security or Emergency Preparedness (NS/EP) telecommunications services and facilities under all conditions, crises, or emergencies; and
- Executing Emergency Support Function 2-Communications (ESF-2) responsibilities under the National Response Framework (NRF).

Homeland Security

National Cybersecurity and Communications Integration Center

NCCIC ORGANIZATION

The NCCIC is comprised of four branches. As mutually supporting, fully integrated elements of the NCCIC, these branches provide the authorities, capabilities, and partnerships necessary to lead a whole-of-nation approach to addressing cybersecurity and communications issues at the operational level.

CYBER AND COMMUNICATIONS COORDINATION AND OPERATIONS INTEGRATION (C^3OI)

Plans, coordinates, and integrates capabilities to synchronize analysis, information sharing, and incident management efforts across the NCCIC's branches and activities.

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM (ICS-CERT)

Reduces risk to the Nation's critical infrastructure by strengthening control systems security through public-private partnerships. ICS-CERT has four focus areas: situational awareness for CIKR stakeholders; control systems incident response and technical analysis; control systems vulnerability coordination; and strengthening cybersecurity partnerships with government departments and agencies.

NATIONAL COORDINATING CENTER FOR TELECOMMUNICATIONS (NCC)

Leads and coordinates the initiation, restoration, and reconstitution of NS/EP telecommunications services or facilities under all conditions. NCC leverages partnerships with government, industry and international partners to obtain situational awareness and determine priorities for protection and response.

UNITED STATES COMPUTER EMERGENCY READINESS TEAM (US-CERT)

Brings advanced network and digital media analysis expertise to bear on malicious activity targeting our nation's networks. US-CERT develops timely and actionable information for distribution to federal departments and agencies, state and local governments, private sector organizations, and international partners. In addition, US-CERT operates the National Cybersecurity Protection System (NCPS), which provides intrusion detection and prevention capabilities to covered federal departments and agencies.

PRIVATE SECTOR EXPERTISE AND RESOURCES

A large majority of our Nation's digital infrastructure is owned and operated by the private sector. Furthermore, cyber threats and malicious activity are pervasive across both public and private sectors. Therefore it is vitally important to incorporate and integrate the private sector into the NCCIC's operations. Critical infrastructure owners and operators are integrated both physically and virtually into the NCCIC during steady state operations, and are fully and appropriately involved in cyber incident response capabilities. Private sector representatives work closely with other NCCIC operational personnel on a daily basis, sharing and receiving actionable information.

ORGANIZATIONAL FLEXIBILITY

A key element of NCCIC operations is its flexibility, which allows the NCCIC and partner entities to adapt rapidly to changing threats. To effectively support response efforts, regardless of size and scope, the NCCIC routinely collaborates with partner organizations on issues related to sharing information, coordinating and de-conflicting actions, conducting analysis, providing assessments, supporting decision activities, and developing common processes and joint plans. The NCCIC's unique organizational structure enables it to swiftly access and leverage the capabilities of multiple public and private sector organizations, allowing it to meet the challenges outlined in the President's Cyberspace Policy Review.

Organizations represented in the NCCIC are:

- DHS components;
- Department of Defense;
- Intelligence community organizations;
- State governments;
- Law enforcement; and
- Private sector and non-governmental partners.

ABOUT DHS CYBER

DHS is responsible for safeguarding our Nation's critical infrastructure from physical and cyber threats that can affect our national security, public safety, and economic prosperity. As DHS's lead agency on cybersecurity, CS&C actively engages the public and private sectors as well as international partners to prepare for, prevent, and respond to catastrophic incidents that could degrade or overwhelm these strategic assets. For more information, please visit www.dhs.gov/cyber.

APPENDIX B: US-CERT SUMMARY

Homeland Security

US-CERT
United States Computer
Emergency Readiness Team

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

The United States Computer Emergency Readiness Team (US-CERT), within the Department of Homeland Security's (DHS) Office of Cybersecurity and Communications (CS&C), was created in September 2003 to help protect the Nation's Internet infrastructure by coordinating defense against and response to cyber-attacks. US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities. As a trusted global leader in cybersecurity, US-CERT builds and leverages partnerships to gain knowledge and raise awareness around the clock.

IMPROVING THE NATION'S CYBERSECURITY POSTURE

As a functional component of the National Cybersecurity and Communications Integration Center (NCCIC), the US-CERT collaborates with Federal, State, local, tribal, and territorial governments, the private sector, the research community, and international entities. Through monitoring, communications, and coordination, US-CERT provides timely and accurate mitigation guidance and serves as the focal point for collaborative cyber awareness and reduction of threats and vulnerabilities. To protect America's cyberspace, US-CERT:

- Administers the National Cyber Alert System to disseminate important cybersecurity warnings and alerts;
- Acts as a trusted third-party to assist in the responsible disclosure of vulnerabilities;
- Coordinates with the law enforcement and intelligence communities and provides the general public with cyber alerts and information;
- Coordinates with partners and customers to achieve shared cyber situational awareness of the Nation's cyber critical infrastructure and key resources;
- Conducts malware analysis and recovery support for government agencies and provides agencies with access to comprehensive digital media analysis capabilities;
- Disseminates actionable situational awareness reports and detection information regarding emerging cyber threats and vulnerabilities and conducts cyber analysis based on situational reporting;
- Provides on-site incident response capabilities to Federal and State agencies and collaborates with domestic and international computer security incident response teams;
- Facilitates information sharing efforts aimed at improving the Nation's cybersecurity posture; and
- Develops and participates in regional, national, and international cybersecurity exercises.

BUILDING SUCCESS THROUGH RELATIONSHIPS

US-CERT is focused on expanding its operational outreach through partnerships with Federal agencies, private sector security vendors, academia, Information Sharing and Analysis Centers (ISACs), State, local, and tribal governments, and international organizations.

US-CERT participates in various information sharing venues, including the Government Forum of Incident Response and Security Teams (GFIRST), ISACs, and corporate computer-security incident response teams.

Homeland Security

US-CERT
United States Computer
Emergency Readiness Team

PROGRAMS AND INITIATIVES

WWW.US-CERT.GOV – Provides the government, private sector, and the public with information needed to protect information systems and infrastructures. The website includes information relevant to current cyber activity, vulnerabilities, recent and archived alerts, events, resources, and security publications.

National Cyber Awareness System (NCAS) – Delivers targeted, timely, and actionable information about cybersecurity topics and threats to users of all technical levels via the US-CERT website and subscriber mailing lists. Visit www.us-cert.gov/cas/signup.html to subscribe or learn more.

US-CERT Secure Portal – Provides a secure, web-based collaborative system to share sensitive cybersecurity information with government and industry partners.

Government Forum of Incident Response and Security Teams (GFIRST) – A community of more than 100 incident response teams from Federal, State, and local agencies working together to secure the Federal Government.

Information Sharing and Analysis Centers (ISACs) – Provides two-way information sharing with private sector partners, as well as State and local governments.

Joint Agency Cyber Knowledge Exchange (JACKE) – A classified forum for Federal departments and agencies to exchange cyber threat and defense information.

National Level Planning – Including the National Cyber Incident Response Plan (NCIRP) which establishes the strategic framework for organizational roles, responsibilities, and actions to prepare for, respond to, and begin to coordinate recovery from a cyber-incident and the National Infrastructure Protection Plan (NIPP) that encourages public and private sectors to collaborate on their respective infrastructure protection activities through a sector partnership model.

Cyber Information Sharing and Collaboration Program (CISCP) – A mechanism for aligning public and private sector coordination. Active Federal participants play a critical role in enabling the program's cross-sector analysis. The program incorporates information from government participants, ISACs, and other critical infrastructure owners and operators, and facilitates the fusion of data through collaboration among CISCP entities to develop and share cross-sector information products through a secure portal.

REPORT CYBER INCIDENTS, VULNERABILITIES, AND PHISHING SCAMS

US-CERT encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, vulnerabilities, and phishing-related scams. Reporting forms can be found at www.us-cert.gov.

Submit cyber threats, incidents, and vulnerabilities via the following methods:

Call: 1-888-282-0870

Email: soc@us-cert.gov

(for encrypted email, US-CERT's PGP key may be downloaded from www.us-cert.gov/pgp/email.html)

ABOUT DHS CYBER

DHS is responsible for safeguarding our Nation's critical infrastructure from physical and cyber threats that can affect national security, public safety, and economic prosperity. As DHS's lead agency on cybersecurity, the Office of Cybersecurity & Communications actively engages the public and private sectors as well as international partners to prepare for, prevent, and respond to catastrophic incidents that could degrade or overwhelm these strategic assets.

For more information on DHS cyber programs, visit www.dhs.gov/cyber.

APPENDIX C: ICS-CERT SUMMARY

Homeland Security

ICS-CERT
Industrial Control Systems
Cyber Emergency Response Team

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), within the Department of Homeland Security's (DHS) Office of Cybersecurity and Communications (CS&C), works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, State, local, and tribal governments and control systems owners, operators, and vendors.

Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.

IMPROVING THE NATION'S CYBERSECURITY POSTURE

As a functional component of the National Cybersecurity and Communications Integration Center (NCCIC), the ICS-CERT is a key component of DHS' *Strategy for Securing Control Systems*. The primary goal of the strategy is to build a long-term common vision where effective risk management of control systems security can be realized through successful coordination efforts.

ICS-CERT leads this effort by:

- Responding to and analyzing control systems-related incidents;
- Conducting vulnerability, malware, and digital media analysis;
- Providing onsite incident response services;
- Providing situational awareness in the form of actionable intelligence;
- Coordinating the responsible disclosure of vulnerabilities and associated mitigations; and
- Sharing and coordinating vulnerability information and threat analysis through information products and alerts.

ONSITE INCIDENT RESPONSE

The ICS-CERT also provides onsite incident response, free of charge, to organizations that require immediate investigation and resolve in responding to a cyber attack. Upon notification of a cyber incident, ICS-CERT will perform a preliminary diagnosis to determine the extent of the compromise. At the customer's request, ICS-CERT can deploy a fly-away team to meet with the affected organization to review network topology, identify infected systems, image drives for analysis, and collect other data as needed to perform thorough follow on analysis. ICS-CERT is able to provide mitigation strategies and assist asset owners/operators in restoring service and provide recommendations for improving overall network and control systems security.

MALWARE LAB

The ICS-CERT operates a malware lab to perform digital media and malware analysis of infected systems. The lab also hosts a representative sample of vendor equipment onsite to give analysts testing capabilities of malware in control system environments. The availability of onsite equipment and software allows ICS -CERT to assess the possible effects of malicious software and consequences a vulnerability may have on critical infrastructure.

Homeland Security

ICS-CERT
Industrial Control Systems
Cyber Emergency Response Team

BUILDING SUCCESS THROUGH PARTNERSHIPS

ICS-CERT coordinates control systems-related security incidents and information sharing with Federal, State, and local agencies and organizations, the intelligence community, and private sector constituents, including vendors, owners and operators, and international and private sector CERTs. The focus on control systems cybersecurity provides a direct path for coordination of activities among all members of the critical infrastructure stakeholder community.

- As an NCCIC component, the ICS-CERT brings industrial control systems security technical and response capabilities to the NCCIC partnership. ICS-CERT performs the work in conjunction with the NCCIC and furthers their overall mission to coordinate defense against and response to cyber attacks across the Nation.
- The ICS-CERT works to reduce risks within and across all critical infrastructure sectors by coordinating efforts among Federal, State, local and tribal governments, as well as control systems owners, operators, and vendors. In addition, the ICS-CERT collaborates with international and private sector CERTs to share control systems related security incidents and mitigation measures.
- ICS-CERT operates an advanced analytics lab that evaluates vulnerabilities and malware (malicious software) associated with control system environments. The lab is able to configure representative samples of control system equipment commonly used within critical infrastructure to support this testing and analysis capability.
- ICS-CERT also brings control systems and cybersecurity technical expertise and incident response capabilities to its partnership with the United States Computer Emergency Readiness Team (US-CERT). Both entities operate side-by-side within the NCCIC to provide a single source of support to critical infrastructure stakeholders.
- ICS-CERT participates with many working groups including the Industrial Control Systems Joint Working Group (ICSJWG) and the Cross-Sector Cyber Security Working Group (CSCSWG). These trusted relationships are leveraged to increase and improve information sharing with critical infrastructure and key resource asset owners and operators as well as the vendor community.

ABOUT DHS CYBER

DHS is responsible for safeguarding our Nation's critical infrastructure from physical and cyber threats that can affect national security, public safety, and economic prosperity. As DHS's lead agency on cybersecurity, the Office of Cybersecurity & Communications actively engages the public and private sectors as well as international partners to prepare for, prevent, and respond to catastrophic incidents that could degrade or overwhelm these strategic assets.

For more information on DHS cyber programs, visit www.dhs.gov/cyber.

To reach a representative of the NCCIC for further information, please contact us at: nccic@dhs.gov or (703) 235-8830.

APPENDIX D: NCC SUMMARY

Homeland Security

National Cybersecurity and Communications Integration Center

THE NATIONAL COORDINATING CENTER FOR COMMUNICATIONS

The National Coordinating Center (NCC) for Communications, within the Department of Homeland Security's (DHS) Office of Cybersecurity and Communications (CS&C), facilitates the exchange among government and industry participants regarding vulnerability, threat, intrusion, and anomaly information affecting the communications infrastructure.

As part of DHS' National Cybersecurity and Communications Integration Center (NCCIC), the NCC continuously monitors national and international incidents and events that may impact emergency communications. Incidents include not only acts of terrorism, but also natural events such as tornadoes, floods, hurricanes and earthquakes. In cases of emergency, the NCC -- through the NCC Watch -- leads emergency communications response and recovery efforts under Emergency Support Function #2 of the National Response Framework.

With much of the nation's cyber infrastructure tied into communications infrastructure, the NCC Watch is also a vital partner to the national cybersecurity effort. The NCC works with both the U.S. Computer Emergency Response Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) to monitor and resolve issues impacting cyber and communications during an emergency.

In January 2000, the White House designated NCC as the Information Sharing and Analysis Center (ISAC) for Communications, in accordance with Presidential Decision Directive-63. The NCC Communications ISAC facilitates the exchange of vulnerability, threat, intrusion, and anomaly information amongst government and industry communications participants.

The NCC cannot perform its vital mission without the cooperation and expertise of its federal and private sector partners. It was the private sector that first recommended the establishment of a centralized government-industry coordination center following the divestiture of AT&T in the early 1980s.

Today, nine Federal Government agencies and over 50 private sector communications and information technology companies routinely share critical communications information and advice in a trusted environment to support the NCC's national security and emergency preparedness communications mission.

NCC FEDERAL PARTICIPANTS

Department of State

Department of Defense

Department of Commerce

Department of Energy

Department of Homeland Security

Federal Communications Commission

Federal Emergency Management Agency

Federal Reserve Board

General Services Administration

Homeland Security

National Cybersecurity and Communications Integration Center

NCC INDUSTRY REPRESENTATIVES

Alcatel Lucent

Alaska Communications

Americom

Association of Public Safety Communications Officials International, Inc. (APCO International)

Artel, Inc.

AT&T

Boeing

CenturyLink

CenturyLink Government

Cincinnati Bell

Cisco Systems

Comcast Cable

COMPTEL

Cox Communications

Computer Sciences Corporation (CSC)

Cellular Telecommunications & Internet Association (CTIA)

Eutelsat America

Fair Point Communications

Frontier Communications

Global Crossing

GlobaFone

Globalstar

Global VSAT

HP Enterprise Services

Hughes

Inmarsat

Intelsat

Internap

Intrado

Juniper Networks

Level 3 Communications

Light Squared

Lockheed Martin

Motorola

National Association of Broadcasters

Nortel Networks

Northrop Grumman

Organization for the Promotion and Advancement of Small Telecommunication Companies

PAETEC

Qualcomm

Raytheon

Research in Motion (RIM)

Science applications International Corporation (SAIC)

SAVVIS, Inc.

SES World Skies

Satellite Industry Association (SIA)

Sprint

TelePacific Communications

T-Mobile

Time Warner Cable

Time Warner Telecom

Tyco Communications

USA Mobility

USTA

VeriSign

Verizon

Verizon Business

Verizon Wireless

ABOUT DHS CYBER

DHS is responsible for safeguarding our nation's critical infrastructure from physical and cyber threats that can affect our national security, public safety, and economic prosperity. As DHS's lead agency on cybersecurity, CS&C actively engages the public and private sectors as well as international partners to prepare for, prevent, and respond to catastrophic incidents that could degrade or overwhelm these strategic assets.

For more information, please visit www.dhs.gov/cyber.

APPENDIX E: ADVANCED MALWARE ANALYSIS CENTER (AMAC) SUMMARY

Homeland Security

US-CERT
United States Computer Emergency Readiness Team

US-CERT ADVANCED MALWARE ANALYSIS CENTER (AMAC)

OVERVIEW

The mission of the United States Computer Emergency Readiness Team (US-CERT) is to improve the Nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation. In addition, US-CERT provides assistance to domestic and international constituents with state-of-the-art incident response capabilities. The Advanced Malware Analysis Center will contribute to US-CERT's strategic goals and mission by analyzing cyber threats and vulnerabilities and providing timely and actionable information.

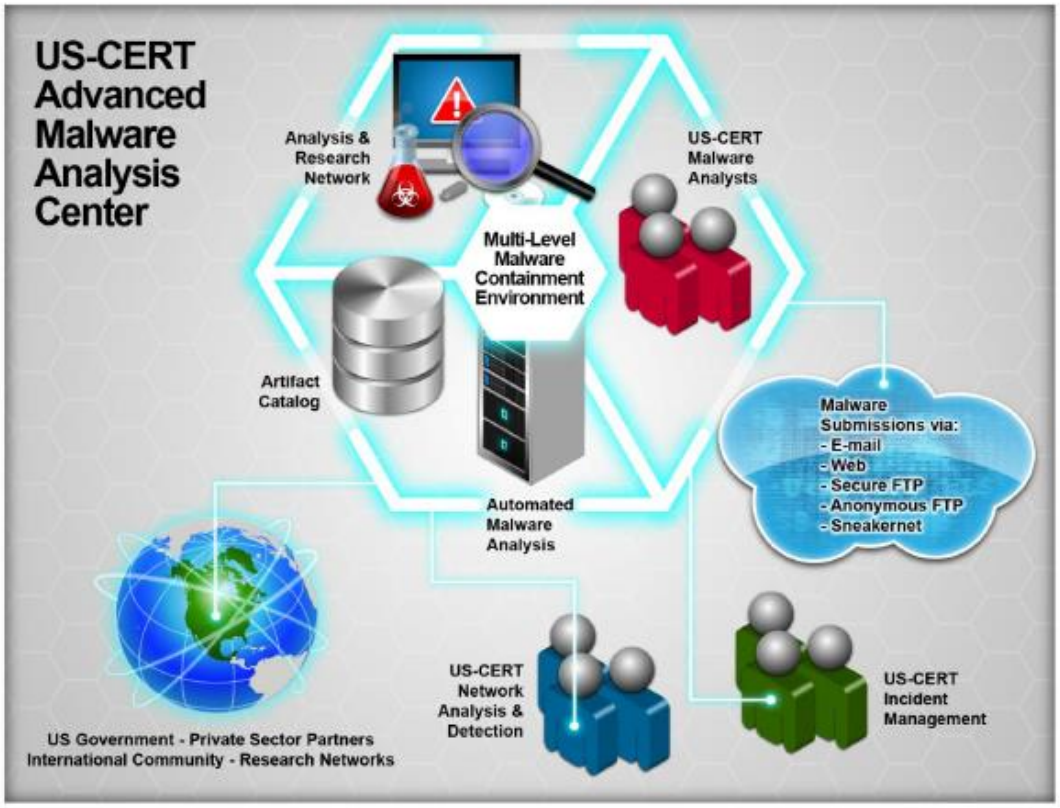
The US-CERT Advanced Malware Analysis Center evolved from a requirement to provide a safe environment to isolate malware for analysis. In October 2011, the facility will expand from a 735 square foot unclassified workspace to a 4350 square feet workspace with enhanced unclassified code analysis and digital media analysis capabilities. With the addition of a Sensitive Compartmented Information Facility, US-CERT will be able to partner with members of the intelligence community, law enforcement, and trusted third parties. The center will provide US-CERT the responsiveness and agility to counter an ever changing stream of cyber threats.

SECURING THROUGH ANALYSIS

The Advanced Malware Analysis Center will be operated by the Digital Analytics Branch of US-CERT. As the only accredited federal malware lab of its kind, it will provide US-CERT with the capability to collect, analyze, and exchange up-to-date malware information 24 hours a day. Elements of its operation are: conducting advanced automated analysis of malware samples; correlating common characteristics across millions of malicious code artifacts; and investigating malware in a safe, secure, and contained environment. US-CERT's Advanced Malware Analysis Center will provide in-depth reporting on malware samples collected and submitted from collaborative partners world-wide.

Homeland Security

US-CERT
United States Computer Emergency Readiness Team



COMPONENTS OF THE ADVANCED MALWARE ANALYSIS CENTER

US-CERT Advanced Malware Analysis Center is structured into 3 sections:

1. DIGITAL MEDIA ANALYSIS (DMA) TEAM
   Analyzes the current state of computer systems, storage mediums, and physical memory of computer systems using forensic investigative tools to identify malware and evidence of malicious activity.
2. CODE ANALYSIS TEAM
   Conducts static analysis and behavior analysis of malicious code types [worms, Trojans, spyware, botnets, rootkits] using standard reverse engineering and debugging tools for malicious artifacts that are extracted from infected systems and submitted to the US-CERT. For security, the DMA network is

malicious artifacts that are extracted from infected systems and submitted to the US-CERT. For security, the DMA network is completely isolated from all other networks. It has two security zones that are separated by a firewall to prevent the live zone from infecting the analysis zone.

3. LAB MANAGEMENT TEAM
   Manages the development of the unclassified and classified labs to ensure that the Malware Analysis Center maintains the appropriate capabilities to support US-CERT's mission.

ADDITIONAL CAPABILITIES

Both the Digital Media Analysis and Code Analysis Teams have fly-away capability to respond to significant cyber security incidents. With an eye to the future, US-CERT will be at the cutting edge of federal cyberspace to quickly produce in-depth analytical reports that help mitigate national-level incidents.

Report Cyber Incidents, Vulnerabilities, and Phishing Scams to US-CERT

US-CERT encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on US-CERT's homepage at www.us-cert.gov.

Submit malware samples to:
virus-submit@us-cert.gov
OR
https://www.malware.us-cert.gov
Note: Do not submit malware samples to soc@us-cert.gov.

To obtain the Public Key for encrypting your e-mail visit: www.us-cert.gov/contact
Telephone: (888) 282-0870

About DHS, NCSD, and NSD

The Department of Homeland Security (DHS) is responsible for safeguarding our Nation's critical infrastructure from physical and cyber threats that can affect our national security,

Homeland Security

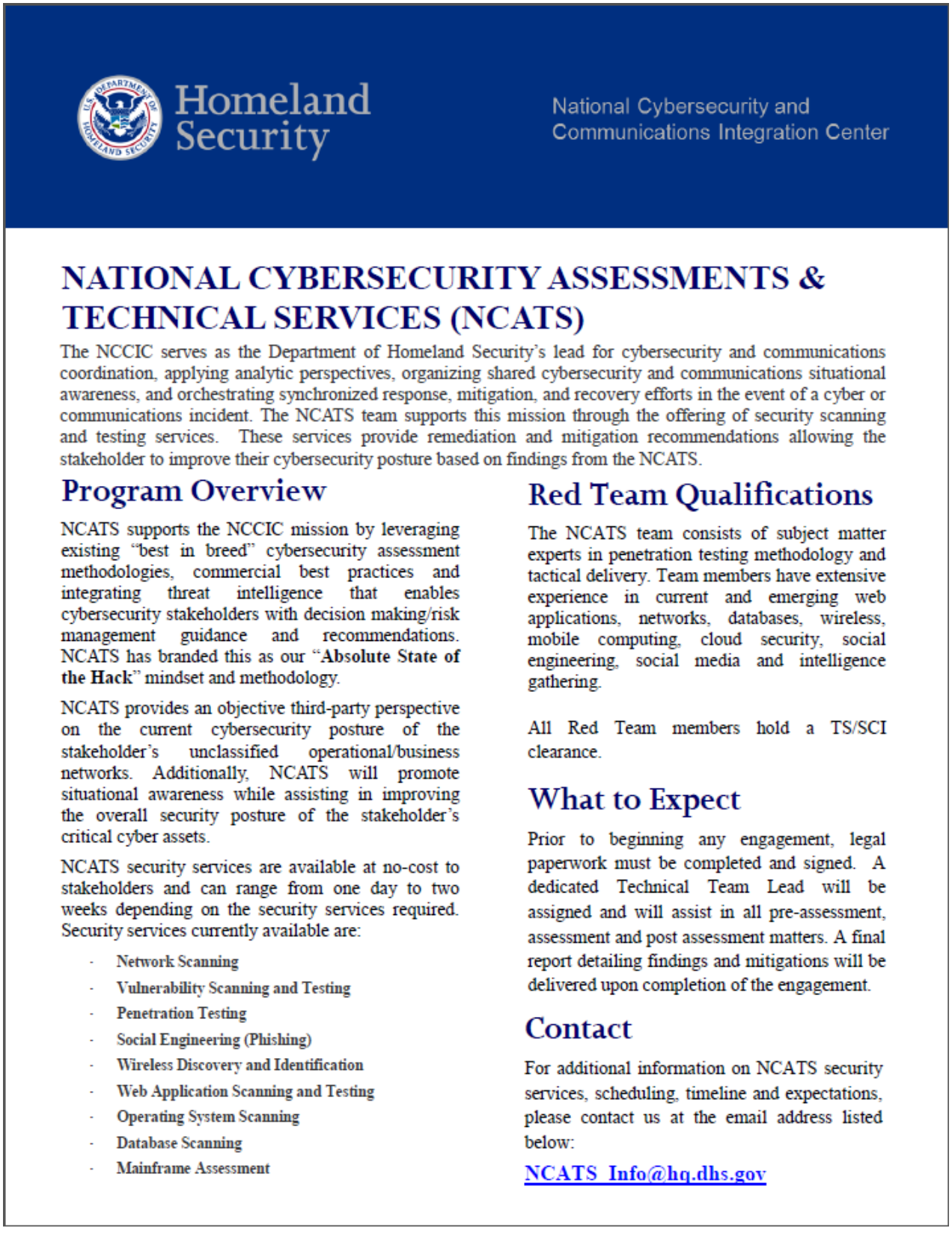
US-CERT
United States Computer Emergency Readiness Team

public safety, and economic prosperity. The National Cyber Security Division (NCSD) is DHS' lead agency for securing cyberspace and our Nation's cyber infrastructure. Furthermore, the Network Security Deployment (NSD) strives to improve the cybersecurity of Federal Government departments, agencies, and partners by delivering the technologies and services needed to fulfill the Office of Cybersecurity and Communications' cybersecurity mission.

For more information, please visit: www.dhs.gov/cyber.

To learn more about US-CERT, visit: www.us-cert.gov or e-mail: info@us-cert.gov.

APPENDIX F: NATIONAL CYBERSECURITY ASSESSMENT AND TECHNICAL SERVICES (NCATS) SUMMARY



Homeland Security

National Cybersecurity and Communications Integration Center

NATIONAL CYBERSECURITY ASSESSMENTS & TECHNICAL SERVICES (NCATS)

The NCCIC serves as the Department of Homeland Security's lead for cybersecurity and communications coordination, applying analytic perspectives, organizing shared cybersecurity and communications situational awareness, and orchestrating synchronized response, mitigation, and recovery efforts in the event of a cyber or communications incident. The NCATS team supports this mission through the offering of security scanning and testing services. These services provide remediation and mitigation recommendations allowing the stakeholder to improve their cybersecurity posture based on findings from the NCATS.

Program Overview

NCATS supports the NCCIC mission by leveraging existing "best in breed" cybersecurity assessment methodologies, commercial best practices and integrating threat intelligence that enables cybersecurity stakeholders with decision making/risk management guidance and recommendations. NCATS has branded this as our "**Absolute State of the Hack**" mindset and methodology.

NCATS provides an objective third-party perspective on the current cybersecurity posture of the stakeholder's unclassified operational/business networks. Additionally, NCATS will promote situational awareness while assisting in improving the overall security posture of the stakeholder's critical cyber assets.

NCATS security services are available at no-cost to stakeholders and can range from one day to two weeks depending on the security services required. Security services currently available are:

- Network Scanning
- Vulnerability Scanning and Testing
- Penetration Testing
- Social Engineering (Phishing)
- Wireless Discovery and Identification
- Web Application Scanning and Testing
- Operating System Scanning
- Database Scanning
- Mainframe Assessment

Red Team Qualifications

The NCATS team consists of subject matter experts in penetration testing methodology and tactical delivery. Team members have extensive experience in current and emerging web applications, networks, databases, wireless, mobile computing, cloud security, social engineering, social media and intelligence gathering.

All Red Team members hold a TS/SCI clearance.

What to Expect

Prior to beginning any engagement, legal paperwork must be completed and signed. A dedicated Technical Team Lead will be assigned and will assist in all pre-assessment, assessment and post assessment matters. A final report detailing findings and mitigations will be delivered upon completion of the engagement.

Contact

For additional information on NCATS security services, scheduling, timeline and expectations, please contact us at the email address listed below:

NCATS_Info@hq.dhs.gov

APPENDIX G: CYBER RESILIENCE REVIEW SUMMARY

Homeland Security

Stakeholder Engagement and
Cyber Infrastructure Resilience

CYBER RESILIENCE REVIEW

The Cyber Security Evaluation program, within the Department of Homeland Security's (DHS) Office of Cybersecurity & Communications (CS&C), conducts a no-cost, voluntary assessment to evaluate and enhance cybersecurity capacities and capabilities within Critical Infrastructure and Key Resources (CIKR) sectors, as well as State, Local, Tribal, and Territorial (SLTT) governments through its Cyber Resilience Review (CRR) process.

OVERVIEW

The goal of the CRR is to develop an understanding and measurement of key cybersecurity capabilities to provide meaningful indicators of an organization's operational resilience and ability to manage cyber risk to its critical services during normal operations and times of operational stress and crisis.

The CRR is based on the CERT Resilience Management Model www.cert.org/resilience/rmm.html, a process improvement model developed by Carnegie Mellon University's Software Engineering Institute for managing operational resilience.

One of the foundational principles of the CRR is the idea that an organization deploys its assets (people, information, technology, and facilities) in support of specific operational missions (i.e., critical services). To ensure the protection and sustainment of its critical services, the CRR seeks to understand an organization's capacities and capabilities in performing, planning, managing, measuring, and defining cybersecurity practices and behaviors in the following ten domains:

1. Asset Management
2. Controls Management
3. Configuration and Change Management
4. Vulnerability Management
5. Incident Management
6. Service Continuity Management
7. Risk Management
8. External Dependency Management
9. Training and Awareness
10. Situational Awareness

The CRR seeks participation from a cross-functional team consisting of representatives from business, operations, security, information technology, and maintenance areas within an organization. This is essential considering no one individual typically has the span of responsibility or knowledge to effectively address every CRR domain. These representatives can be personnel who have the following roles and responsibilities within the organization:

- IT policy & procedures (e.g., Chief Information Security Officer)
- IT security planning & management (e.g., Director of Information Technology)
- IT infrastructure (e.g., network/system administrator)
- IT operations (e.g., configuration/change manager)
- Business operations (e.g., operations manager)
- Business continuity & disaster recovery planning (e.g., BC/DR manager)
- Risk analysis (e.g., enterprise/operations risk-manager)

APPENDIX H: USSS ELECTRONIC CRIMES TASK FORCE (ECTF) SUMMARY

Homeland Security

National Cybersecurity and Communications Integration Center

UNITED STATES SECRET SERVICE (USSS)

Electronic Crimes Task Forces and Working Groups

In 2001, the USA PATRIOT Act, enacted by Congress, directed the Secret Service to establish nationwide Electronic Crimes Task Forces to combine the resources of academia; the private sector; and local, state and federal law enforcement agencies to "prevent, detect and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems."

It is the goal of the Electronic Crimes Task Forces to establish, promote and continue a robust public / private partnership based on the U.S. Secret Service's historic strategic alliances with federal, state and local law enforcement agencies, private industry and academic institutions in order to respond, confront and suppress cyber crime, malicious uses of cyberspace and threats to cyber security that endanger the integrity of our nation's financial payments systems and threats against our nation's critical infrastructure.

The ECTFs focus on several types of investigations to include: network intrusions, hacking attacks, phishing schemes, skimming, access device fraud, carding portals, wire fraud, use of malicious software and other computer-related offenses.

Memberships in our ECTFs include approximately 300 academic partners; 2,700 international, federal, state and local law enforcement partners; and 3,100 private sector partners.

*This represents individual contacts affiliated with approximately 5,000 separate academic, corporate and law enforcement organizations.

Today, the Secret Service's 31 ECTFs have successfully dismantled some of the largest known cybercriminal organizations targeting our financial critical infrastructure. Since 2001, the Secret Service ECTFs have arrested over 10,000 suspects for cybercrime-related violations and prevented over $13 billion in potential losses to victims.

U.S. Secret Service Electronic Crimes Task Forces

Domestic

Atlanta, Birmingham, Baltimore, Boston, Buffalo, Charlotte, Chicago, Cleveland, Columbia, Dallas, Houston, Las Vegas, Los Angeles, Louisville, Miami, Memphis, Minneapolis, New Orleans, New York, Oklahoma/Tulsa, Orlando, Philadelphia, Phoenix, Pittsburgh, San Francisco, Seattle, St. Louis, Washington, D.C.

Europe

London, England; Rome, Italy

To report any malicious activities, please visit http://www.secretservice.gov/ectf.shtml , and select an ECTF location.

NCCIC Resource and Capabilities Guide