Safeguarding and Securing Cyberspace

Our economic vitality and national security depend today on a vast array of interdependent and critical networks, systems, services, and resources. We know this interconnected world as cyberspace, and without it we cannot communicate, travel, power our homes, run our economy, or obtain government services. Its benefits are tremendous. Yet as we migrate even more of our economic and societal transactions to cyberspace, these benefits come with increasing risk. For this reason, safeguarding and securing cyberspace has become one of the homeland security community's most important missions.

Cybersecurity Assessment Tools

Cyber Resiliency Review (CRR) is an assessment that the Cyber Security Evaluation Program offers to measure and enhance the implementation of key cybersecurity capacities and capabilities of critical infrastructure and key resources (CIKR). The purpose of the CRR is to gather information regarding cybersecurity performance from specific CIKR in order to gain an understanding of the relationships and impacts of CIKR performance in protecting critical infrastructure operations. The results can be used to evaluate a provider independent of other assessments, used with regional studies to build a common perspective on resiliency, and used to examine systems-of-systems (i.e., large and diverse operating and organizing models). The key goal of the CRR is to ensure that core process-based capabilities exist, are measureable, and are meaningful as predictors for an organization's ability to manage cyber risk to national critical infrastructure. For more information about the CRR, contact the CSEP program at CSE@dhs.gov.

Cybersecurity Evaluation Program (CSEP) conducts voluntary cybersecurity assessments across all 18 CIKR sectors, within state governments and large urban areas. CSEP affords critical infrastructure sector participants a portfolio of assessment tools, techniques, and analytics, ranging from those that can be self-applied to those that require expert facilitation or mentoring outreach. The CSEP works closely with internal and external stakeholders to measure key performances in cybersecurity management. The Cyber Resiliency Review is being deployed across all 18 Critical Infrastructure sectors, state, local, tribal, and Territorial governments. For more information, visit www.dhs.gov/xabout/structure/editorial_0839.shtm or contact CSE@dhs.gov.

Cybersecurity Evaluation Tool (CSET) is a desktop software tool that guides users through a step-by-step process for assessing the cyber security posture of their industrial control system and enterprise information technology networks. CSET is available for download or in DVD format. To learn more or download a copy, visit http://www.us-cert.gov/control_systems/satool.html. To obtain a DVD copy, send an e-mail with your mailing address to CSET@dhs.gov.

Cybersecurity Vulnerability Assessments through the Control Systems Security Program (CSSP) provide on-site support to critical infrastructure asset owners by assisting them to perform a security self-assessment of their enterprise and control system networks against industry accepted standards, policies, and procedures. To request on-site assistance, asset owners may e-mail CSSP@dhs.gov.

Industrial Control Systems (ICS) Technology Assessments provide a testing environment to conduct baseline security assessments on industrial control systems, network architectures, software, and control system components. These assessments include testing for common vulnerabilities and conducting vulnerability mitigation analysis to verify the effectiveness of applied security measures. To learn more about ICS testing capabilities and opportunities, e-mail CSSP@dhs.gov.

Information Technology Sector Risk Assessment (ITSRA) provides an all-hazards risk profile that public and private IT Sector partners can use to inform resource allocation for research and development and other protective measures which enhance the security and resiliency of the critical IT Sector functions. For more information, see http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf or contact ncsd_cipcs@hq.dhs.gov.

Cybersecurity Incident Resources

Current Cybersecurity Activity is a regularly updated summary of the most frequent, high-impact types of security incidents currently being reported to the US-CERT. For more information, see http://www.us-cert.gov/current/ or contact info@us-cert.gov (888) 282-0870.

Cyber Investigation Section (CIS) CIS is designed to target and proactively investigate major international criminals. This goal is accomplished through a combination of long-term undercover operations, close partnerships with other US government agencies, and consistently refined strategic targeting. In conjunction with this unique role, CIS has prototyped numerous advanced technical systems that allow for the integration and re-use of diverse forms of evidence from all US jurisdictions and foreign partners. Also included under this unit are analysts and Criminal Research Specialists who focus on foreign language websites, money laundering activities, and digital/electronic currency. For more information, see www.secretservcie.gov/ectf.shtml.

Cyber Forensics the products developed through this program are cyber forensic analysis devices used by law enforcement in the daily investigation of criminal and terrorist activity and the tools developed allow investigators to visualize, analyze, share, and present data derived from cell phones, GPS devices, computer hard drives, networks, personal data assistants, and other digital media. For more information, contact SandT-CyberLiaison@hq.dhs.gov.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) The ICS-CERT focuses on control system security across all critical infrastructure and key resource (CIKR) sectors. The ICS-CERT supports asset owners with reducing the risk of cyber attacks by providing alerts and advisories, conducting incident response activities, and performing technical analysis of malware, artifacts, and vulnerabilities. For more information, visit http://www.us-cert.gov/control_systems/ics-cert or contact ICS-CERT at ics-cert@dhs.gov.

National Computer Forensics Institute (NCFI) Is the result of a partnership between the Secret Service and the State of Alabama. The goal of this facility is to provide a national standard of training on a variety of electronic crimes investigations. This program will offer state and local law enforcement officers the training necessary to conduct computer forensics examinations, respond to network intrusion incidents, and conduct basic electronic crimes investigations. The NCFI will also train prosecutors, and judges on the importance of computer forensics to criminal investigations. This training acts as a force multiplier for the Secret Service and other federal law enforcement agencies, thus reducing the volume of cyber crime cases impacting the federal judicial process. For more information, see www.ncfi.usss.gov.

National Cyber Alert System the US-CERT National Cyber Awareness System offers a variety of up-to-date information on general cybersecurity topics, threats and vulnerabilities via subscription lists and feeds for alerts, bulletins, and tips. For more information, visit http://www.us-cert.gov/cas/ or contact info@us-cert.gov (888) 282-0870.

U.S. Computer Emergency Readiness Team (US-CERT) Monthly Activity Summary provides monthly updates made to the National Cyber Alert System. This includes current activity updates, technical and non-technical alerts, bulletins, and tips, in addition to other newsworthy events or highlights. For more information, see http://www.us-cert.gov/security-publications/#reports; contact info@us-cert.gov (888) 282-0870.

U. S. Computer Emergency Readiness Team (US-CERT) Operations Center Report cybersecurity incidents (including unexplained network failures), the discovery of malicious code, and vulnerability information at https://forms.us-cert.gov/report/. Contact the US-CERT Operations Center at soc@us-cert.gov (888) 282-0870.

U.S. Computer Emergency Readiness Team (US-CERT) Vulnerability Notes Database includes technical descriptions of each vulnerability, as well as the impact, solutions and workarounds, and lists of affected vendors. For more information, see http://www.kb.cert.org/vuls or contact info@us-cert.gov (888) 282-0870.

U.S. Computer Emergency Readiness Team (US-CERT) Security Publications provide subscribers with free, timely information on cybersecurity vulnerabilities, the potential impact of those vulnerabilities, and actions required to mitigate the vulnerability and secure their computer systems. For more information, see http://www.us-cert.gov/security-publications/ or contact info@us-cert.gov (888) 282-0870.

Cybersecurity Technical Resources

Cybersecurity Advisors (CSAs) act as principal field liaisons in cybersecurity and provide a federal resource to regions, communities, and businesses. Their primary goal is to assist in the protection of cyber components essential within the nation's critical infrastructure and key resources (CIKR). Equally important is their role in supporting cybersecurity risk management efforts at the state and local homeland security initiatives. CSAs will work with established programs in state and local areas, such as Protective Security Advisors, FEMA emergency management personnel, and fusion center personnel. For more information, contact the program at CSE@dhs.gov.

Cybersecurity Research and Development Center (CSRDC) DHS S&T utilizes CSRDC to focus cyber security research and development efforts and to involve the best practices and personnel from academic, private industry, federal and national laboratories. For more information about this and other DHS S&T projects, workshop information and presentations, cybersecurity news, events and outreach information, see http://www.cyber.st.dhs.gov/ or contact SandT-Cyber-Liaison@hq.dhs.gov.

Cybersecurity in the Retail Subsector Webinar provides retail employees and managers with an overview of the cyber threats and vulnerabilities facing the industry. The webinar also reviews the types of cyber systems and infrastructure used by the retail industry and steps that retail personnel can take to address the unique vulnerabilities to those cyber resources. The webinar is available on HSIN-CS at https://connect.hsin.gov/p78334832/. For more information contact CFSTeam@hq.dhs.gov.

Cybersecurity Public Trends and Analysis Report provides awareness of the cyber security trends as observed by the U.S. Computer Emergency Readiness Team (US-CERT). The analysis in this report is based on incident information that has been reported to US-CERT, incidents identified by US-CERT, and public/private sector information identified when correlating and analyzing the data. For more information contact US-CERT at info@us-cert.gov (888) 282-0870.

Control Systems Security Program (CSSP) Cybersecurity Training is provided through an instructor-led introductory course for control system and IT professionals or a five-day advanced course which includes hands-on instruction in an actual control system environment. On-line introductory cybersecurity courses are also available. For more information, see http://www.us-cert.gov/control_systems/cstraining.html or contact CSSP@dhs.gov.

Control Systems Security Program (CSSP) reduces industrial control system risks within and across all critical infrastructure and key resource sectors. CSSP coordinates cybersecurity efforts among federal, state, local, and tribal governments, as well as industrial control system owners, operators, and vendors. CSSP provides many products and services that assist the industrial control system stakeholder community to improve their cybersecurity posture and implement risk mitigation strategies. To learn more about the CSSP, visit http://www.us-cert.gov/control_systems/ or e-mail CSSP@dhs.gov.

Critical Infrastructure Protection Cyber Security (CIP-CS) leads efforts with public and private sector partners to promote safe, secure, and resilient U.S. cyber infrastructure. Major elements of the CIP-CS program include: managing and strengthening cyber critical infrastructure partnerships with public and private entities in order to effectively implement risk management and cybersecurity strategies; teaming with cyber critical infrastructure partners in the successful implementation of cybersecurity strategies; and promoting effective cyber communications processes with partners that result in a collaborative, coordinated approach to cyber awareness. For more information, contact CIP-CS at ncsd_cipcs@hq.dhs.gov.

Cybersecurity Education and Workforce Development Program (CEWD) fosters effective cybersecurity education and workforce development programs by facilitating the availability of professionals qualified to support the nation's cybersecurity needs. To support national cybersecurity workforce development, CEWD developed the IT Security Essential Body of Knowledge (EBK), an umbrella framework that links competencies and functional perspectives to IT security roles to accurately reflect a national perspective. For more information, see http://www.us-cert.gov/ITSecurityEBK/.

Cybersecurity in the Emergency Services Sector Webinar is a one-hour overview of the types of cyber systems and infrastructure that the Emergency Services Sector utilizes. The webinar also address the threats and vulnerabilities to those cyber resources and is available on the Homeland Security Information Network – Critical Sectors (HSIN-CS) Emergency Services Sector Portal. For access and more information, contact ESSTeam@hq.dhs.gov.

Cybersecurity in the Retail Sector Webinar This webinar will provide retail employees and managers with an overview of the cyber threats and vulnerabilities facing the industry. Viewers of the Webinar will gain a heightened sense of the importance of strengthening cybersecurity in the retail workplace. The Webinar also will review the types of cyber systems and infrastructure used by the retail industry and steps that retail personnel can take to address the unique vulnerabilities to those cyber resources. Also includes One-pager/invitation. . The Webinar is available on HSIN-CS at https://connect.hsin.gov/p78334832/. For more information, please contact the Commercial Facilities SSA at CFSTeam@dhs.gov.

Cybersecurity Information Products and Recommended Practices provide current cybersecurity information resources and recommend security practices to help industry understand emerging control systems cyber security issues and mitigate vulnerabilities. This information will help users reduce their exposure and susceptibility to cyber attacks and exploits. For a complete list and access to cybersecurity information products, visit http://www.us-cert.gov/control_systems/csdocuments.html. For more information, contact CSSP@dhs.gov.

Domain Name System Security Extensions (DNSSEC) Deployment Coordinating Initiative provides cryptographic support for domain name system (DNS) data integrity and authenticity. DHS sponsors a community-based, international effort to transition the current state of DNSSEC to large-scale global deployment, including sponsorship of the DNSSEC Deployment Working Group, a group of experts active in the development or deployment of DNSSEC. It is open for anyone interested in participation. The DNSSEC website contains articles, published research papers, DNSSEC tools, case studies, workshop information, and presentation materials. See http://www.dnssec-deployment.org/.

Industrial Control System Cybersecurity Standards and References provide an extensive collection of cybersecurity standards and reference materials as a ready resource for the industrial control system stakeholder community. To view the collection, visit http://www.us-cert.gov/control_systems/csstandards.html. For more information, contact CSSP@dhs.gov.

Information Technology Sector Specific Plan (IT SSP) outlines the IT Sector security partners' joint implementation of the NIPP risk management framework. It describes an approach for identifying, assessing, prioritizing, and protecting critical IT Sector functions, establishing shared IT Sector goals and objectives, and aligning initiatives to meet them. To view the IT SSP, visit http://www.dhs.gov/xlibrary/assets/nipp-ssp-information-tech-2010.pdf. For more information, contact ncsd_cipcs@hq.dhs.gov.

The National Cyber Security Division's (NCSD) Critical Infrastructure Protection Cyber Security (CIP-CS) program developed a flexible, repeatable, and reusable cyber risk management approach to help CIKR sectors, state and local governments, and other public and private sector organizations manage cyber critical infrastructure risk. This approach—the Cybersecurity Assessment and Risk Management Approach (CARMA)—incorporates lessons from a

wide variety of cyber risk management activities. CARMA is a comprehensive, functions-based risk management strategy that focuses on cyber critical infrastructure and effectively identifies, assesses, and manages shared risks. For more information, email ncsd_cipcs@hq.dhs.gov.

Network Security Information Exchange (NSIE) The NCS and the National Security Telecommunications Advisory Committee (NSTAC) recommended the establishment of an Industry-government partnership to reduce the vulnerability of the Nations' telecommunications systems to electronic intrusion. The NCS and NSTAC formed separate government and Industry Network Security Information Exchanges to share ideas on technologies and techniques for addressing and mitigating the risks to the public network and its supporting infrastructures. For more information, visit http://www.ncs.gov/nstac/reports/fact_sheet/NSTAC_08.pdf.

National Vulnerability Database (NVD) is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security-related software flaws, misconfigurations, product names, and impact metrics. For more information, visit http://nvd.nist.gov/ or contact nvd@nist.gov.

The Protected Repository for the Defense of Infrastructure against Cyber Threats (PREDICT) facilitates the accessibility of computer and network operational data for use in cyber defense research and development through large-scale research datasets. PREDICT allows partners to pursue technical solutions to protect the public and private information infrastructure. It also provides researchers and developers with real network data to validate their technology and products before deploying them online. Within this project, the Los Angeles Network Data Exchange and Repository (LANDER), Network Traffic Data Repository to Develop Secure Information Technology Infrastructure, Routing Topology and Network Reliability Dataset Project, and Virtual Center for Network and Security Data serve as data set collectors and hosts. The PREDICT Data Coordinating Center helps manage and coordinate the research data repository. For more information visit https://www.predict.org or contact PREDICT-contact@rti.org.

Roadmap to Enhance Cyber Systems Security in the Nuclear Sector The Roadmap to Enhance Cyber Systems Security in the Nuclear Sector describes coordinated activities to improve cyber systems security in the Nuclear Sector. It provides nuclear control and cyber systems vendors, asset owners and operators, and relevant government agencies, with a common vision, goals, and objectives for cyber systems security in the sector. It also provides milestones to focus specific efforts and activities for achieving the vision, goals, and objectives over the next 10 to 15 years, addressing the Nuclear Sector's most urgent challenges, as well as its longer-term needs to reduce the cyber security risk to nuclear industrial cyber systems. For more information, please contact the NPPD/IP Nuclear SSA at NuclearSSA@hq.dhs.gov.

Roadmap to Secure Control Systems in the Chemical Sector The Roadmap to Secure Control Systems in the Chemical Sector describes a plan for voluntarily improving cybersecurity in the Chemical Sector. It brings together Chemical Sector stakeholders, government agencies, and asset owners and operators with a common set of goals and objectives. For more information, please contact the NPPD/IP Chemical SSA at ChemicalSector@hq.dhs.gov.

Software Assurance (SwA)

Automating Software Assurance Under SwA sponsorship, MITRE, in collaboration with government, industry, and academic stakeholders, is improving the measurability of security through enumerating baseline security data, providing standardized languages as means for accurately communicating the information, and encouraging sharing of this information with users by developing repositories (see Making Security Measurable: http://buildsecurityin.us-cert.gov/swa/measurable.html). MITRE issues electronic newsletters on the following technologies employed in automating SwA: Common Vulnerabilities and Exposures (CVE); Common Weakness Enumeration (CWE); Common Attack Pattern Enumeration and Classification (CAPEC); Open Vulnerability and Assessment Language (OVAL); and Malware Attribute Enumeration and Characterization (MAEC).

Software Assurance Program (SwA) Software Assurance is the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted and that software applications function in the intended manner. Grounded in the National Strategy to Secure Cyberspace, the SwA Program develops practical guidance and tools, and promotes research and development of secure software engineering. Resources including articles, webinars, podcasts, and tools for software security automation and process improvement are constantly updated at the SwA Community Resources and Information Clearinghouse located at https://buildsecurityin.us-cert.gov/swa/. For more information, contact software.assurance@dhs.gov.

Software Assurance (SwA) Forum and Working Group Sessions Four times per year, under the co-sponsorship of organizations in DHS, the Department of Defense (DoD), and the National Institute of Standards and Technology (NIST), the SwA Forum and Working Group Sessions provide a venue for participants to share their knowledge and expertise in software security while interacting and networking with key leaders in industry, government, and academia. During the Forums, the SwA Program offers free tutorials. Several of these tutorials are available on line from the Software Engineering Institute's Virtual Training Environment (VTE) at https://www.vte.cert.org/vteweb/go/3719.aspx.

Software Assurance (SwA) Resources To support SwA in higher education, SwA and the Software Engineering Institute (SEI) have developed Software Assurance Curriculum Materials (https://buildsecurityin.us-cert.gov/swa/mswa.html) which are freely available for download. This curriculum is formally recognized by the Institute of Electrical and Electronics Engineers (IEEE) and the Association for Computing Machinery (ACM). At the Forum and Working Group Sessions, SwA distributes CDs of SwA resources. Included on the CDs are guides, reports, and brochures on numerous topics such as: SwA Capability Benchmarking Documents (https://buildsecurityin.us-cert.gov/swa/proself_assm.html); SwA Ecosystem Page (https://buildsecurityin.us-cert.gov/swa/ecosystem.html); FAQs and Fact Sheets on SwA Forums and Working Groups (https://buildsecurityin.us-cert.gov/swa/faq.html); Whitepapers from the Software Assurance Community (https://buildsecurityin.us-cert.gov/swa/ttpe_research.html); Evaluating and Mitigating Software Supply Chain Security Risk, May 2010 (https://buildsecurityin.us-cert.gov/swa/downloads/MitigatingSWsupplyChainRisks10tn016.pdf); and SwA Pocket Guide Series - free, downloadable documents on critical software assurance topics (https://buildsecurityin.us-cert.gov/swa/pocket_guide_series.html).

Software Assurance (SwA) Email Newsletter provides excellent updates and new information related to the SwA program. To subscribe to the newsletter, email listproc@nist.gov and put 'subscribe' in the subject line and 'subscribe sw.assurance' in the body of the email.

Software Assurance (SwA) Checklist for Software Supply Chain Risk Management SwA developed and deployed the "SwA Checklist for Software Supply Chain Risk Management" which identifies common elements of publicly available software assurance models. The SwA Checklist provides a consolidated view of current software assurance goals and best practices in the context of an organized SwA initiative. The checklist includes mappings between the SwA Checklist practices and practices identified in existing SwA maturity models and related capability maturity models. This mapping provides a valuable reference for those wishing to improve their software assurance capabilities. For more information, see https://buildsecurityin.us-cert.gov/swa/proself_assm.html#checklist.

Software Assurance (SwA) Outreach As part of an extensive outreach effort, the SwA participates in conferences and webinars with the International Information Systems Security Certification Consortium $(ISC)^2$, the Information Systems Security Association, Open Web Application Security Project (OWASP), and other organizations interested in application security. More about SwA relevant webinars is available on the BSI and CRIC websites. Please visit https://buildsecurityin.us-cert.gov/swa/webinars.html for more information. Moreover, SwA supports online communities of interest, such as the Software Assurance Education Discussion Group on LinkedIn (http://www.linkedin.com/groups?mostPopular=&gid=3430456) and the Software Assurance Mega-Community (http://www.linkedin.com/groups?home=&gid=1776555&trk=anet_ug_hm)

The Top 25 Common Weakness Enumerations (CWE) In cooperation with the System Administration, Audit, Network Security (SANS) Institute, SwA and MITRE issued the report, "Improve Security and Software Assurance: Tackle the CWE Top 25 – The Most Dangerous Programming Errors." The Top 25 CWEs represent the most significant exploitable software constructs that have made software so vulnerable. Communicating and addressing these problematic issues will serve to improve software security, both during development and while in operation. Read more and see the list of "Top 25 CWE Programming Errors" at https://buildsecurityin.us-cert.gov/swa/cwe/.