

Safeguarding and Securing Cyberspace

The Department has the lead for the federal government for securing civilian government computer systems, and works with industry and state, local, tribal and territorial governments to secure critical infrastructure and information systems. The Department works to: analyze and reduce cyber threats and vulnerabilities; distribute threat warnings; and coordinate the response to cyber incidents to ensure that our computers, networks, and cyber systems remain safe.

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 measurable, 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 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.

Emergency Services Sector Cyber Risk Assessment (ESS-CRA) is the first ESS-wide cyber risk assessment completed under the National Infrastructure Protection Plan (NIPP) framework, and it will inform collaborative and synchronized management of cyber risk across the sector. The ESS-CRA is intended to provide a risk profile that ESS partners can use to enhance the security and resilience of the ESS disciplines. By increasing the awareness of risks across the public and private sector domains, the ESS-CRA serves as a foundation for ongoing national-level collaboration to enhance the security and resilience of the ESS disciplines. The ESS-CRA is an initial effort to assess ESS cyber risks across the ESS disciplines and serves as a baseline of national-level risk. The

assessment addresses those operational or strategic risks to the ESS infrastructure that are of national concern based upon the knowledge and subject matter expertise of those participating in the sector's risk assessment activities. The ESS-CRA describes an effort that required resources and coordination from across all disciplines of ESS in order to assess cyber risks to ESS critical infrastructure. This risk assessment provides the basis for an ESS cyber risk management plan or roadmap that will ensure that Federal resources are applied where they offer the most benefit for mitigating risk by lowering vulnerabilities, deterring threats, and minimizing the consequences of attacks and other incidents. The report also encourages a similar risk-based allocation of resources within State and local entities and the private sector. For more information, please contact essteam@hq.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 <http://www.secretservice.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.uss.gov.

National Cyber Awareness 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

The Cross-Sector Cyber Security Working Group (CSCSWG) enhances cybersecurity protection efforts by identifying opportunities to improve cross-sector cybersecurity coordination; highlighting cyber dependencies and interdependencies; and sharing cybersecurity products and findings. Each month, more than 100 members attend the CSCSWG to exchange cybersecurity information, ideas, concepts, and activities. To review and resolve specific, critical cross-sector cybersecurity issues, member-driven, ad-hoc CSCSWG groups may be created that encourage bi-directional collaboration, dialogue, and debate. In the past, members have created subgroups to address information sharing, performance metrics, and incentivizing cybersecurity implementation. In 2011, a subgroup was created to review, discuss, and provide recommendations to strengthen a healthy and resilient “cyber ecosystem.” CSCSWG members have also contributed to several national cybersecurity policy documents since its inception, including coordinating on aspects of the Comprehensive National Cybersecurity Initiative, reviewing and commenting on the Obama Administration’s 60 Day Policy Review, and the resulting Cyberspace Policy Review. For more information, email ncsd_cipcs@hq.dhs.gov.

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.

Cyber Exercise Program (CEP) was established in 2004 to strengthen the reliability and resiliency of the Nation's critical cyber infrastructure through the development, design, and conduct of scenario-based cyber exercises. The CEP can build a Cyber Tabletop Exercise Package (CTEP) for most any critical infrastructure/key resource sector and has already co-produced CTEPs for the Chemical, Critical Manufacturing, and the Healthcare and Public Health Sectors. The CTEP provides organizations all the materials needed to plan and conduct a discussion-based cyber exercise. The CTEP includes two scenarios designed to help assess security policies and procedures for both the "business" and "operational" aspects of an organization. Highly customizable, it gives the planner the flexibility to use organizational goals and objectives, or choose goals and objectives included in the package. Also included in the package are planning guides, templates, checklists to guide and track the planning process, Situation Manuals, and post-exercise instructions. For more information, please contact CEP@DHS.GOV.

Cybersecurity Strategy Development, led by the National Cyber Security Division's (NCSA) Critical Infrastructure Protection Cyber Security (CIP-CS) program helps sectors and States outline and develop robust cybersecurity strategies by providing the basic framework that can be tailored to needs of the individual sector or State. The detailed guidance outlines key sections of a cybersecurity strategy and provides tips for developing each section. It also provides general information on the purpose and benefits of developing a strategy that can be used to

communicate and obtain buy-in for the effort among stakeholders and leadership. A cybersecurity strategy provides sectors and State governments with an actionable plan to manage both strategic and operational cyber risks to their core business capabilities and products and services. By outlining specific goals, objectives, and milestones, a sector or State can continuously enhance their overall cybersecurity posture and adapt to the changing cyber risk landscape. For more information, email ncsd_cipcs@hq.dhs.gov.

Department of Homeland Security Science and Technology Directorate Cyber Security Division (DHS S&T CSD) DHS S&T CSD's mission is to develop and transition new technologies, tools, and techniques to protect and secure systems, networks, infrastructure, and users, improving the foundational elements of our nation's critical infrastructure and the world's information infrastructure; and, to provide coordination and research and development leadership across federal, state, and municipal government; international partners; the private sector; and academia to improve cybersecurity research infrastructure. DHS S&T CSD frequently works with the private sector to develop requirements and engage transition partners for the tools, technologies and techniques that result from CSD's work. For more information about CSD and its specific 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 Gaming Subsector Webinar focused on cybersecurity threats, vulnerabilities, and best practices specific to the gaming and casino industry. More than 100 gaming industry representatives participated in the Webinar, which was designed to raise awareness of cybersecurity within the Gaming Subsector. The Critical Infrastructure Protection Cybersecurity (CIP CS) program and Office of Intelligence and Analysis (I&A) discussed some of the latest cyber threats specific to the Gaming Subsector and steps industry can take to improve their cyber resilience. These steps include

managing employees to mitigate insider threats, communicating with gaming machine vendors about vulnerabilities, securing newly digital IP surveillance systems, and conducting cybersecurity assessments. For more information, email ncsd_cipcs@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.

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.

The Cybersecurity Assessment and Risk Management Approach (CARMA), created by the National Cyber Security Division's (NCSA) 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. CARMA incorporates lessons from a wide variety of cyber risk management activities. CARMA accounts for the virtual and distributed nature of cyber critical infrastructure and the complexity of the missions and services it supports; considers strategic security goals and can guide all levels of cyber risk efforts; and allows infrastructure owners and operators to integrate their established cyber risk frameworks into the approach or use the approach as a foundation for broader enterprise risk management efforts. 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.

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 addresses 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.

Cybersecurity Webinars, as an information sharing mechanism, can increase the level of participation and activity among public and private sector stakeholders by engaging them in a cybersecurity discussion. The National Cyber Security Division's (NCSD) Critical Infrastructure Protection Cyber Security (CIP-CS) Program can help plan, coordinate, and execute a cybersecurity webinar in partnership with sector stakeholders by identifying webinar topics to address goals and objectives; assisting the host organization with determining participants, timeframe, and speakers; developing a webinar outline; inviting other Department of Homeland Security (DHS) components to participate and coordinate on topics of interest; and working with the sponsoring sector or organization to provide follow-up materials. CIP-CS has partnered with the Commercial Facilities and Emergency Services Sectors to produce webinars. For more information, email ncsd_cipcs@hq.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/sector-specific-plans>. 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 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 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, mis-configurations, product names, and impact metrics. For more information, visit <http://nvd.nist.gov/> or contact nvd@nist.gov.

Open Source Infrastructure Cyber Read File

compiles important cybersecurity and cyber infrastructure news articles across CIKR sectors and provides a repository of cybersecurity open source information. The Read Files are intended to increase awareness of cybersecurity issues—thus aiding sectors during strategic cybersecurity risk management planning. Modeled on the Department of Homeland Security's Daily Open Source Infrastructure Report, the monthly Open Source Infrastructure Cyber Read File focuses on cybersecurity and cyber infrastructure. Articles are drawn from open source news resources and are organized by date and the sector(s) they affect. In the Open Source Infrastructure Cyber Read File, CIP CS applies knowledge of how issues could

inform sectors' strategic planning efforts by including contextual information in addition to the news article. The additional context helps increase understanding of how cybersecurity impacts critical infrastructure protection efforts. Sector-Specific Agencies (SSAs) and other organizations, including State and Federal government agencies, may share the Read File with their stakeholders, many of whom may not be aware of cybersecurity issues relevant to their activities. For more information, email ncsd_cipcs@hq.dhs.gov.

The Research Data Repository Project is the only freely-available legally collected repository of large-scale datasets containing real network and system traffic. A primary impetus of this project is to also provide a streamlined legal framework to centralize a controlled distribution of datasets, while protecting researchers, data providers and data hosts. The intent is to accelerate design, production, and evaluation of next-generation cyber security solutions, including commercial products. Data providers legally provide the data to be shared through the repository, data hosts provide the infrastructure to store the repository data and transfer it to authorized recipients, and the coordinating center provides a centralized mechanism for cataloging available data and manages the submission and review of data requests. The goal of the distributed structure is to provide secure, centralized access to multiple sources of data and promote data sharing while protecting the privacy of the data producers and the security of their networks and data. PREDICT continually adds new data containing the latest cybersecurity attacks so that the research community will have the most recent information to help improve the quality of research results. 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)

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.

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 Security Automation & Measurement: <http://buildsecurityin.us-cert.gov/swa/measurable.html>). Sponsored by the Software Assurance Program, MITRE issues electronic newsletters and information 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). Structured Threat Information eXpression (STIX) is a quickly evolving, collaborative community-driven effort to define and develop a language to represent structured threat information. The STIX language is meant to convey the full range of cyber threat information and strives to be fully expressive, flexible, extensible, automatable, and as human-readable as possible. It is actively being adopted or considered for adoption by a wide range of cyber threat-related organizations and communities around the world. All interested parties are welcome to participate in evolving STIX as part of its open, collaborative community and leverage the upcoming STIX web site and collaborative forums. For more information, see http://www.mitre.org/work/tech_papers/2010/10_1420/10_1420.pdf.

Resilient Software Software Assurance promotes the security and resilience of software across the development, acquisition, and operational lifecycle; as such, SwA is scoped to address Trustworthiness, Dependability (correct and predictable execution), Conformance, and Survivability. The focus on Resilience and Survivability enables stakeholders to understand and proactively take action to design, build, acquire, and operate software and software-enabled services with knowledge that software must be able to operate in non-benign environments. Moreover, if compromised, damage to the software will be minimized and it will recover quickly to an

acceptable level of operating capacity; it's "rugged." Several initiatives have focused on developing rugged software that is attack-aware and self-defending. See <https://buildsecurityin.us-cert.gov/swa/resilient.html> for details.

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. The gatherings are unique in focus by bringing together private sector stakeholders to protecting key information technologies, most of which are enabled and controlled by software. 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 ([\[cert.gov/swa/tpe_research.html\]\(https://buildsecurityin.us-cert.gov/swa/tpe_research.html\)\); 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 \(\[https://buildsecurityin.us-cert.gov/swa/pocket_guide_series.html\]\(https://buildsecurityin.us-cert.gov/swa/pocket_guide_series.html\)\).](https://buildsecurityin.us-</p>
</div>
<div data-bbox=)

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_lm)

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/>.