

DHS Cyber Security Resources Catalog

Saturday, June 12, 2010

Contributed By:

[Marjorie Morgan](#)



From [The Internet Security Alliance](#)

The Department of Homeland Security (DHS) has released a "Private Sector Resources Catalog" collecting training, publications, guidance, alerts, newsletters, programs, and services available to the private sector.

This is the first such effort to encompass all of DHS and represents a commitment to facilitate public access and increase transparency.

The publication recognizes the diversity of the private sector and includes resources for academia, nonprofits, NGOs, and businesses large and small.

DHS has repeatedly stated the important role played by these actors in our nation's homeland security and has worked to strengthen partnerships and increase engagement at the local, state, and federal levels.

Earlier this year, DHS released the Quadrennial Homeland Security Review report to Congress outlining an enterprise approach to homeland security in which multiple partners including the private sector share roles and responsibilities in upholding the public safety and well-being of the United States.

Cybersecurity and Communications (CS&C)

The Office of Cybersecurity and Communications (CS&C) is responsible for enhancing the security, resiliency, and reliability of the nation's cyber and communications infrastructure. 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. http://www.dhs.gov/xabout/structure/gc_1185202475883.shtm

CS&C Training and Education

Control Systems Security Program (CSSP) Instructor-Lead Cybersecurity Training is provided through an introductory course for IT professionals or a 5-day advanced course which includes hands-on instruction in an actual control system environment. For more information, see http://www.us-cert.gov/control_systems/cstraining.html, or contact CSSP@dhs.gov.

Cyber Education and Workforce Development Program (CEWD) As cyber threats and their sophistication increase, the demand for qualified IT security professionals increases as well. In response, the National Cyber Security Division's Cyber Education and Workforce Development program (CEWD) developed the IT Security Essential Body of Knowledge (EBK). The IT Security EBK is an umbrella framework that links competencies and functional perspectives to IT security roles to accurately reflect a national perspective. See <http://www.us-cert.gov/ITSecurityEBK/>.

CS&C Publications and Guidance

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. An interactive site with recommended practices for control system networks can be found at <http://csrp.inl.gov/>. For more information, contact CSSP@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, see http://www.us-cert.gov/reading_room/index.html#news. Contact US-CERT at info@us-cert.gov, (888) 282-0870

Cyber Security 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 in DVD format. To learn more, visit http://www.us-cert.gov/control_systems/satool.html. To obtain a DVD copy of CSET, send an e-mail with your mailing address to CSET@dhs.gov.

Emergency Communications Guidance Documents and Methodologies The DHS Office of Emergency Communications develops stakeholder-driven guidance documents and methodologies to support emergency responders across the Nation as they plan for and implement emergency communications initiatives. These resources identify and promote best practices on improving statewide governance, developing standard operating procedures, managing technology, supporting training and exercises, and encouraging usage of interoperable communications, among other topics. Each is available publicly and is updated as needed. Examples include: Establishing Governance to Achieve Statewide Communications

Interoperability and the Formal Agreement and Standard Operating Procedure Template Suite. For more information, contact the Office of Emergency Communications at oeq@hq.dhs.gov or visit <http://www.safecomprogram.gov>.

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. The collection provides a one-stop location for accessing papers, reports, references, and standards associated with industrial control system cybersecurity. To view the collection, visit http://www.us-cert.gov/control_systems/csstandards.html. For more information, contact CSSP@dhs.gov.

Information Technology Sector Risk Assessment (ITSRA) The National Cyber Security Division (NCSA), in partnership with public and private sector partners from the **IT Sector Coordinating Council (IT SCC)** and the **IT Government Coordinating Council (IT GCC)**, released the baseline ITSRA in 2009. The 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. By increasing the awareness of risks across the public and private sectors, the Baseline Risk Assessment is the foundation for ongoing national-level collaboration to enhance the security and resiliency of the critical IT Sector functions. See http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf. For more information, contact ncsd_cipcs@hq.dhs.gov.

Information Technology Sector Specific Plan (IT SSP) and the National Cyber Security Division (NCSA), in partnership with private sector members of the IT Sector, has developed the IT SSP to outline 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/IT_SSP_5_21_07.pdf. For more information, contact ncsd_cipcs@hq.dhs.gov.

National Emergency Communications Plan (NECP) is a strategic plan that sets goals and identifies key national priorities to enhance governance, planning, technology, training and exercises, and disaster communications capabilities. The NECP establishes specific national priorities to help State and local jurisdictions improve communications interoperability by adopting a series of goals and milestones that measure interoperability achievements over a period of years beginning in 2008, and ending in 2013. In order to successfully implement the NECP, increased collaboration between the public and private sector will be needed. As a result, the plan establishes specific initiatives and milestones to increase such collaboration. For more information, see http://www.dhs.gov/xlibrary/assets/national_emergency_communications_plan.pdf or contact the Office of Emergency Communications, oeq@hq.dhs.gov.

National Interoperability Field Operations Guide (NIFOG) is a technical reference for radio technicians responsible for radios that will be used in disaster response applications, and for

emergency communications planners. The NIFOG includes rules and regulations for use of nationwide and other interoperability channels, frequencies and channel names, and other reference material, formatted as a pocket-sized guide for radio technicians to carry with them. The NIFOG can be accessed online at <http://www.npstc.org/psdocs.jsp#nifog>. For more information, contact the Office of Emergency Communications, oeq@hq.dhs.gov.

SAFECOM Guidance for Federal Grant Programs The Department of Homeland Security Office of Emergency Communications, in coordination with the Office for Interoperability and Compatibility, develops the annual SAFECOM Guidance for Federal Grant Programs. Although SAFECOM is not a grant-making body, the guidance outlines recommended allowable costs and applications requirements for Federal grant programs providing funding for interoperable emergency communications. The guidance is intended to ensure that Federal grant funding for interoperable communications aligns with national goals and objectives and ensures alignment of State, local, and tribal investment of Federal grant funding to statewide and national goals and objectives. See http://www.safecomprogram.gov/NR/rdonlyres/31A870C0-0C9D-4C29-86F8-147D61AF25CF/0/FY_2010_SAFECOM_Recommended_Guidance_111809_Final.pdf. For more information, contact the Office of Emergency Communications at oeq@hq.dhs.gov.

U.S. Computer Emergency Readiness Team (US-CERT) Monthly Activity Summary summarizes general activity as well as updates made to the National Cyber Alert System each month. This includes current activity updates, technical and non-technical alerts, bulletins, and tips, in addition to other newsworthy events or highlights. See http://www.us-cert.gov/reading_room/index.html#news, contact US-CERT at 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 action required to mitigate the vulnerability and secure their computer systems. See http://www.us-cert.gov/reading_room, contact US-CERT at info@us-cert.gov, (888) 282-0870.

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

CS&C Alerts and Newsletters

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. See <http://www.us-cert.gov/current/>, contact US-CERT at info@us-cert.gov, (888) 282-0870.

Critical Infrastructure Information Notices are intended to provide warning to critical infrastructure owners and operators when a particular cyber event or activity has the potential to impact critical infrastructure computing networks. This document is distributed only to those

parties who have a valid "need to know," a direct role in securing networks or systems that enable or support U.S. critical infrastructures. Access is limited to a secure portal (<https://portal.us-cert.gov>) and controlled distribution list. For more information, contact the US-CERT Secure Operations Center at soc@us-cert.gov; (888) 282-0870.

National Cyber Alert System offers a variety of information for users with varied technical expertise including **Technical Cybersecurity Alerts and Bulletins** or more general-interest pieces such as Cybersecurity Alerts and Tips on a variety of cyber-related topics. See <http://www.uscert.gov/cas/alldocs.html>. Contact US-CERT at info@us-cert.gov, (888) 282-0870.

CS&C Technical Assistance

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.

Cyber Resiliency Review (CRR) is an assessment offered by the **Cyber Security Evaluation Program** 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 CRR serves as a repeatable cyber review, while allowing for an evaluation of enterprise-specific cybersecurity capabilities. 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.

Cyber Security 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 Security Evaluation Program (CSEP) conducts voluntary cybersecurity assessments across all 18 CIKR Sectors, within state governments, and for large urban areas. CSEP affords CIKR 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, in alignment with the DHS National Infrastructure Protection Plan (NIPP), works closely with and coordinates efforts 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 (as denoted by DHS), state, local, tribal, and territorial governments. For more information, visit www.dhs.gov/xabout/structure/editorial_0839.shtm or contact the program at CSE@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 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.

CS&C Programs and Services

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 an assured 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 cip_cs@dhs.gov.

Global Supply Chain Risk Management (GSCRM) Program provides recommendations to standardize and implement risk management processes for acquiring information and communications technologies (ICT) for the federal government, and processes to reduce the threat of attacks to federal ICT through the supply chain. Your organization can help with this initiative by applying sound security procedures and executing due diligence to provide integrity and assurance through the vendor supply chain. For more information, visit http://www.dhs.gov/files/programs/gc_1234200709381.shtm or contact the Global Supply Chain Program at Kurt.Seidling@hq.dhs.gov.

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.

SAFECOM Program is a communications program which provides research, development, testing, and evaluation, guidance, tools, and templates on interoperable communications-related issues to local, Tribal, State, and Federal emergency response agencies. The SAFECOM web site provides members of the emergency response community and other constituents with information and resources to help them meet their communications and interoperability needs. The site offers comprehensive information on topics relevant to emergency response communications and features best practices that have evolved from real-world situations. See <http://www.safecomprogram.gov>, contact SAFECOM@dhs.gov.

Software Assurance Program Software Assurance (SwA) is the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the intended manner. Grounded in the **National Strategy to Secure Cyberspace**, the Department of Homeland Security's Software Assurance Program spearheads the development of practical guidance and tools and promotes research and development of secure software engineering, examining a range of development issues from new methods that avoid basic programming errors to enterprise systems that remain secure when portions of the system software are compromised. Resources including articles, webinars, podcasts, and tools can be found at the SwA Community Resources and Information Clearinghouse located at <https://buildsecurityin.us-cert.gov/swa/>. For more information, contact software.assurance@dhs.gov.

DHS will regularly update the catalog in order to publicize new resources and increase awareness. To download the catalog, [click here](#).

The Internet Security Alliance (ISA) is a unique multi-sector trade association which provides thought leadership and strong public policy advocacy as well as business and technical services to its membership. The ISA represents enterprises from the aviation, banking, communications, defense, education, financial services, insurance, manufacturing, security, and technology industries. ISA's mission is to integrate advanced technology with the realistic business needs of its members and enlightened public policy to create a sustained system of cyber security