FEDERAL CYBER RESOURCES

# CYBER RESILIENCE REVIEW (CRR)

The CRR is a no-cost, voluntary, non-technical assessment to evaluate an organization’s operational resilience and cybersecurity practices. The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals. The CRR assesses enterprise programs and practices across a range of 10 domains including risk management, incident management, service continuity and others. The assessment is designed to measure existing organizational resilience as well as provide a gap analysis for improvement based on recognized best practices.

# CYBER SECURITY EVALUATION TOOL (CSET)

The Cyber Security Evaluation Tool (CSET®) is a Department of Homeland Security (DHS) product that assists organizations in protecting their key national cyber assets. It was developed under the direction of the DHS Industrial Control System Cyber Emergency Response Team (ICS-CERT) by cybersecurity experts and with assistance from the National Institute of Standards and Technology (NIST). This tool provides users with a systematic and repeatable approach for assessing the security posture of their cyber systems and networks. It includes both high-level and detailed questions related to all industrial control and IT systems.

# DEPARTMENT OF HOMELAND SECURITY (DHS)

The Office of Cybersecurity and Communications (CS&C) works with state and local government as well as private sector partners to minimize the impact of cybersecurity incidents. Two of CS&C’s National Cybersecurity and Communications Integration Center components, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and United States Computer Emergency Readiness Team (US-CERT) work to mitigate cybersecurity incidents in close coordination with public and private sector partners.

ICS-CERT provides onsite support to owners and operators of critical infrastructure, including incident response, forensic analysis and site assessments. ICS-CERT also provides tools and training designed to increase stakeholder awareness of the threats posed to industrial control systems.

The ICS-CERT website provides various resources for owners and operators of critical infrastructure and the industrial control systems that operate many of the key functions of their facilities, such as the SCADA system. The website contains links to resources such as alerts, advisories, newsletters, training and recommended practices, as well as a large list of standards and references.

The ICS-CERT website can be found here: <https://ics-cert.us-cert.gov/>. ICS cyber incidents can be reported to: ics-cert@hq.dhs.gov.

# DEPARTMENT OF HOMELAND SECURITY PROTECTIVE SECURITY ADVISORS AND CYBER SECURITY ADVISORS

The Department of Homeland Security (DHS) Protective Security Advisor (PSA) program offers critical infrastructure owner/operators a conduit to many free services such as security training, site assessments and assistance with local exercise coordination. Colorado’s PSA is Joe O’Keefe, .Joseph.OKeefe@HQ.DHS.GOV.

There is also a regionally based Cyber Security Advisor (CSA) that functions in the same capacity for cybersecurity-specific issues. Denver will be getting its own CSA in the coming year.

More information on the PSA program may be found here: [http://www.dhs.gov/protective-security-](http://www.dhs.gov/protective-security-advisors)  [advisors](http://www.dhs.gov/protective-security-advisors).

# iGUARDIAN

The FBI recently released the iGuardian portal as a pilot program designed to give companies a designated location to report cyber threats they’ve encountered. Initially, the program will be open only to members of the InfraGard Network (see above). The iGuardian portal offers a one-stop-shop for cyber incident reporting. Reports received by iGuardian will go to the local FBI office and the FBI may follow up with the reporting entity. More information on becoming an InfraGard member can be found here: [www.infragard.org/](https://www.infragard.org/).

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

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce risks within and across all criti[cal infrastructure sectors](http://www.dhs.gov/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.

Complete list of DHS resources at [www.dhs.gov/sites/default/files/publications/Policy-](http://www.dhs.gov/sites/default/files/publications/Policy-PSO/private_sector_resource_catalog_December_2012.pdf)  [PSO/private\_sector\_resource\_catalog\_December\_2012.pdf](http://www.dhs.gov/sites/default/files/publications/Policy-PSO/private_sector_resource_catalog_December_2012.pdf)

# INFRAGARD

InfraGard is a Federal Bureau of Investigation (FBI) program that began in the Cleveland Field Office in 1996. It was a local effort to gain support from the information technology industry and academia for the FBI’s investigative efforts in the cyber arena. The program expanded to other FBI Field Offices, and in 1998 the FBI assigned national program responsibility for InfraGard to the former National Infrastructure Protection Center (NIPC) and to the Cyber Division in 2003. InfraGard and the FBI have developed a relationship of trust and credibility in the exchange of information concerning various terrorism, intelligence, criminal and security matters. InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the FBI and the private sector.

The goal of InfraGard is to promote ongoing dialogue and timely communication between members and the FBI. InfraGard members gain access to information that enables them to protect their assets and in turn give information to government that facilitates its responsibilities to prevent and address terrorism and other crimes. Membership is free and open to all critical infrastructure owners and operators.

More information, including information on membership, can be found here: [www.infragard.org/](https://www.infragard.org/).

# INFORMATION SHARING AND ANALYSIS CENTERS (ISACs)

The mission of the National Council of ISACs (NCI) is to advance the physical and cybersecurity of the critical infrastructures of North America by establishing and maintaining a framework for valuable interaction between and among the ISACs and with government. Members of the Council are the

individual Information Sharing and Analysis Centers (ISAC) that represent their respective sectors. Main website: [www.isaccouncil.org.](http://www.isaccouncil.org/)

# NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER (NCCIC)

The NCCIC, within the Office of Cybersecurity and Communications, serves as a centralized location where operational elements involved in cybersecurity and communications reliance are coordinated and integrated. NCCIC partners include all federal departments and agencies; state, local, tribal and territorial governments; the private sector; and international entities. The center’s activities include providing greater understanding of cybersecurity and communications situation awareness vulnerabilities, intrusions, incidents, mitigation and recovery actions. Main website: [www.dhs.gov/about-national-cybersecurity-communications-integration-center](http://www.dhs.gov/about-national-cybersecurity-communications-integration-center).

Cyber incidents can be reported to the NCCIC watch desk at: NCCIC\_ WatchandWarning@hq.dhs.gov.

# REGIONAL RESILIENCY ASSESSMENT PROGRAM (RRAP)

The RRAP evaluates critical infrastructure on a regional level to examine vulnerabilities, threats and potential consequences from an all-hazards perspective, identifying dependencies, interdependencies, cascading effects, resilience characteristics and gaps. Each year, the Department selects RRAP projects with input and guidance from federal and state partners. RRAP projects, which are voluntary and non- regulatory, focus on specific infrastructure sectors within geographic areas and address a range of hazards that may have significant regional and national consequences.

# SANS

The Twenty Critical Security Controls have already begun to transform security in government agencies and other large enterprises by focusing their spending on the key controls that block known attacks and find the ones that get through. Agreed upon by a powerful consortium which included NSA, US Cert, DoD JTF-GNO, the Department of Energy Nuclear Laboratories, Department of State, DoD Cyber Crime Center plus the top commercial forensics experts and pen testers that serve the banking and critical infrastructure communities, the automation of these top 20 controls will radically lower the cost of security while improving its effectiveness.