DHS Cyber Security Evaluations: Summary – 1

Name	Cyber Resilience Review (CRR)	Cyber Infrastructure Survey Tool (C-IST)	Supply Chain Risk Management Review	Onsite Cyber Security Evaluation Tool (CSET) Assessment
Purpose and Value Proposition	Identify cyber security management capabilities and maturity	To calculate a comparative analysis and valuation of protective measures in-place	Identify external dependencies and the risks associated	Provides a detailed, effective, and repeatable methodology for assessing control systems security – while encompassing an organization's infrastructure, policies, and procedures
Scope	Critical Service view	Critical Cyber Service view	Organization / Business Unit	Industrial Control Systems
Time to Execute	5 to 6 Hours	2 ½ to 4 Hours	2 to 2 ½ Hours	8 Hours (1 Business Day)
Information Sought	Capabilities and maturity indicators in 10 security domains	Protective measures in-place	Third-party security requirements and contract management info	Industrial control system's core functions, infrastructure, policies, and procedures
Preparation	Short, 1-hour questionnaire plus planning calls	Planning call to scope evaluation	Planning call to scope evaluation	Coordinated via Email. Planning calls if requested
Participants	IT/Security Manager, Continuity Planner, and Incident Responders	IT/Security Manager	IT / Security Manager with Contract Management	Control system operators/ engineers, IT, policy/ management personnel, and subject matter experts
Delivery By	SECIR/Stakeholder Risk Assessment & Mitigation	SECIR/Stakeholder Risk Assessment & Mitigation	SECIR/Stakeholder Risk Assessment & Mitigation	NCCIC/ICS-CERT

DHS Cyber Security Evaluations: Summary – 2

Name	ICS-CERT Design Architecture Review (DAR)	ICS Network Architecture Verification and Validation (NAVV)	Network Risk and Vulnerability Assessment (RVA)	Cyber Hygiene (CH) Evaluation
Purpose	Supports the cybersecurity design via investigative analysis, production, and maintenance of control systems and ICS components	Provides analysis and base-lining of ICS communication flows, based upon a passive (non-intrusive) collection of TCP Header Data	Perform penetration testing and security services to identify risks and vulnerabilities within IT systems, networks and applications	Identify public-facing Internet security risks, through service enumeration and vulnerability scanning
Scope	Industrial Control Systems/ Network Architecture	Industrial Control Systems/ Network Architecture/ Network Traffic	Organization / Business Unit / Network-Based IT Service	Public-Facing, Network-Based IT Service
Time to Execute	2 Days (8 Hours Each Day)	Variable (Hours to Days)	Variable (Days to Weeks)	Variable (Hours to Continuous)
Information Sought	Network design, configurations, interdependencies, and its applications	Network traffic header-data to be analyzed with Sophia Tool	Network, Database, Application scope and/or access to be tested with various security tools	Network service and vulnerability information
Preparation	Coordinated via Email. Planning calls	Coordinated via Email. Planning calls	Formal rules of engagement and extensive pre-planning	Formal rules of engagement and extensive pre-planning
Participants	Control system operators/ engineers, IT personnel, and ICS network, architecture, and topologies SMEs	Control system operators/ engineers, IT personnel, and ICS network, architecture, and topologies SMEs	IT/Security Manager and Network Administrators	IT/Security Manager and Network Administrators
Delivered By	NCCIC/ICS-CERT	NCCIC/ICS-CERT	NCCIC/NCATS	NCCIC/NCATS

ABOUT DHS CYBER

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