February 2015

Homeland Security

DHS Cyber Security & Resilience Resources:

Cyber Preparedness, Risk Mitigation, & Incident Response

Cyber Security Advisor Program
Office of Cybersecurity & Communications
National Protection and Programs Directorate
U.S. Department of Homeland Security

DHS CYBER COORDINATION AND INCIDENT RESPONSE

A Wide Range of Offerings for Critical Infrastructure

- National Cybersecurity and Communications Integration Center (NCCIC)
  - US-CERT Operations Center
    - Remote and On-Site Assistance
    - Malware Analysis
    - Incident Response Teams
  - ICS-CERT Operations Center
    - ICS-CERT Malware Lab
    - Cyber Security Evaluation Tool
    - Incident Response Teams
  - NCATS
    - Cyber Hygiene service
    - Risk and Vulnerability Assessment
- US-CERT
  - National Cyber Awareness System
  - Vulnerability Notes Database
  - Security Publications
- Control Systems Security Program
  - Cybersecurity Training
  - Information Products and Recommended Practices
- Cyber Exercise Program
- Cyber Security Evaluations Program
  - Cyber Resilience Review
  - Cyber Infrastructure Survey Tool
- Cyber Security Advisors
- Protective Security Advisors

Homeland Security

Critical Infrastructure Cyber Community (C^3)

Website:

http://www.us-cert.gov/ccubedvp

General C3 inquiries:
ccubedvp@hq.dhs.gov

C3 VP (Pre-Recorded) Webinar:
https://share.dhs.gov/p4k4bp51kx7/

- DHS launched the C^3 Program in February 2014 to complement the launch of the NIST CSF
- The C^3 Voluntary Program helps sectors and organizations that want to use the CSF by connecting them to existing cyber risk management capabilities provided by DHS, other U.S. Government organizations, and the private sector.
- The C3 website (http://www.us-cert.gov/ccubedvp) describes the various programs DHS offers to critical infrastructure partners, including Federal, State, local, and private sector organizations
- Many of the programs described on the following slides can also be found on the website

Homeland Security

Incident Reporting

NCCIC provides real-time threat analysis and incident reporting capabilities

- 24x7 contact number: 1-888-282-0870; https://forms.us-cert.gov/report/

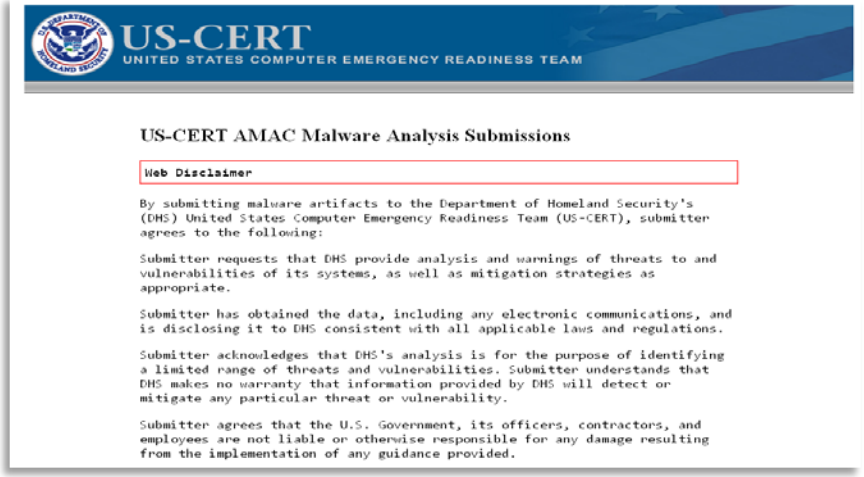
When to Report:

If there is a suspected or confirmed cyber attack or incident that:

- ❖ Affects core government or critical infrastructure functions;
- ❖ Results in the loss of data, system availability; or control of systems;
- ❖ Indicates malicious software is present on critical systems

Malware Submission Process:

- Please send all submissions to the Advance Malware Analysis Center (AMAC) at: submit@malware.us-cert.gov
- Must be provided in password-protected zip files using password “infected”
- Web-submission: https://malware.us-cert.gov


US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

US-CERT AMAC Malware Analysis Submissions

Web Disclaimer

By submitting malware artifacts to the Department of Homeland Security's (DHS) United States Computer Emergency Readiness Team (US-CERT), submitter agrees to the following:

Submitter requests that DHS provide analysis and warnings of threats to and vulnerabilities of its systems, as well as mitigation strategies as appropriate.

Submitter has obtained the data, including any electronic communications, and is disclosing it to DHS consistent with all applicable laws and regulations.

Submitter acknowledges that DHS's analysis is for the purpose of identifying a limited range of threats and vulnerabilities. Submitter understands that DHS makes no warranty that information provided by DHS will detect or mitigate any particular threat or vulnerability.

Submitter agrees that the U.S. Government, its officers, contractors, and employees are not liable or otherwise responsible for any damage resulting from the implementation of any guidance provided.

Homeland Security

DHS CYBER PREPAREDNESS EVALUATIONS

DHS CYBER SECURITY EVALUATIONS - SUMMARY - 1

Name	Cyber Resilience Review (CRR)	Cyber Infrastructure Survey Tool (C-IST)	Supply Chain / External Dependency Management (EDM) Review	Onsite Cyber Security Evaluation Tool (CSET) Assessment
Purpose	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	8 Hours (1 business day)	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 call(s)	Planning call to scope evaluation	Planning call to scope evaluation	Coordinated via Email. Planning call(s) 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.

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 and deep technical analysis of enterprise IT systems and an organization's external resistance to specific IT risks	Identify public-facing Internet security risks, at a high-level, 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.	Low-level options and recommendations for improving IT network and system security	High-level network service and vulnerability information
Preparation	Coordinated via Email. Planning call(s).	Coordinated via Email. Planning call(s).	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

CRR Self-Assessment Package

- Released in February 2014 to complement the launch of the NIST CSF.
- The CRR Self-Assessment Kit allows organizations to conduct a review without outside facilitation.
- Contains the same questions, scoring, and reporting as the facilitated assessment.
- The kit contains the following resources:
  - Method Description and User Guide
  - Complete CRR Question Set with Guidance
  - Self-Assessment Package (automated toolset)
  - CRR to NIST CSF Crosswalk
- **CRR Self-Assessment Kit website:**
  - http://www.us-cert.gov/ccubedvp/self-service-crr

Homeland Security

Cyber Security Evaluation Tool (CSET®)

- Stand-alone software application
- Self-assessment using recognized standards
- Tool for integrating cybersecurity into existing corporate risk management strategy

CSET Download:

http:/us-cert.gov/control_systems/csetdownload.html

Homeland Security

DHS Cyber Resources – Operations Focused

- **National Cybersecurity and Communications Integration Center (NCCIC)**
  - Serves as a national center for reporting and mitigating communications and cybersecurity incidents. http://www.dhs.gov/about-national-cybersecurity-communications-integration-center
  - Provides:
    - 24x7 real-time threat analysis and incident reporting capabilities, at 1-888-282-0870
    - Malware Submission Process:
      - Please send all submissions to: submit@malware.us-cert.gov
      - Must be provided in password-protected zip files using password "infected"
      - Web-submission: https://malware.us-cert.gov
    - ICS-CERT Training: http://ics-cert.us-cert.gov/cscalendar.html
- **Cyber Security Evaluations Program (cse@hq.dhs.gov)**
  - Provides no-cost, voluntary cyber security evaluations and assessments, including:
    - Cyber Resilience Review (CRR)
      - One-day, facilitated evaluation focused on critical IT services and the security management process
    - Cyber Security Evaluation Tool (CSET)
      - Stand-alone software application, used as a self-assessment against recognized standards and a tool for creating a baseline of cybersecurity practices
      - Downloadable at: http:/us-cert.gov/control_systems/csetdownload.html

Contact Information

Evaluation Inquiries
cse@hq.dhs.gov

General Inquiries
cyberadvisor@hq.dhs.gov

Contact Information	
Bradford Willke Program Manager, Cyber Security Advisor Program	Bradford.Willke@hq.dhs.gov
Sean McCloskey Acting Branch Chief, Stakeholder Risk Assessment & Mitigation	Sean.McCloskey@hq.dhs.gov

Department of Homeland Security
National Protection and Programs Directorate
Office of Cybersecurity and Communications