UNITED STATES (EST)| VIRTUAL VIA ZOOM

March 2-4, 2021

**REFERENCES**

**U.S. Cybersecurity and Infrastructure Security Agency**

**Critical Infrastructure Sectors**

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. This site offers guidance on the essential critical infrastructure workforce, as well as resources for each of the 16 sectors.

<https://www.cisa.gov/critical-infrastructure-sectors>

**Ransomware Guidance and Resources**

Looking to learn more about this growing cyber threat? The NEW Ransomware Guide is a great place to start. The Guide, released in September 2020, represents a joint effort between CISA and the Multi-State Information Sharing and Analysis Center (MS-ISAC). The joint Ransomware Guide includes industry best practices and a response checklist that can serve as a ransomware-specific addendum to organization cyber incident response plans. In January 2021, CISA unveiled the Reduce the Risk of Ransomware Campaign to raise awareness and instigate actions to combat this ongoing and evolving threat. The campaign is a focused, coordinated and sustained effort to encourage public and private sector organizations to implement best practices, tools and resources that can help them mitigate ransomware risk.

[www.cisa.gov/ransomware](http://www.cisa.gov/ransomware)

**CISA Industrial Control Systems Security Offerings**

Industrial Control Systems (ICS) are important to supporting US critical infrastructure and maintaining national security. ICS owners and operators face threats from a variety of adversaries whose intentions include gathering intelligence and disrupting National Critical Functions.To support the ICS community's cyber risk management efforts, CISA offers ICS owners and operators a wide range of products, services, and capabilities. Click on the CISA Industrial Control Systems Security Offerings and Capabilities fact sheet below to learn more.

[www.cisa.gov/publication/ics-security-offerings](http://www.cisa.gov/publication/ics-security-offerings)

**Cybersecurity Best Practices For Industrial Control Systems**

Industrial Control Systems (ICS) are important to supporting US critical infrastructure and maintaining national security. ICS owners and operators face threats from a variety of adversaries whose intentions include gathering intelligence and disrupting National Critical Functions. As ICS owners and operators adopt new technologies to improve operational efficiencies, they should be aware of the additional cybersecurity risk of connecting operational technology (OT) to enterprise information technology (IT) systems and Internet of Things (IoT) devices.

<https://www.cisa.gov/publication/cybersecurity-best-practices-for-industrial-control-systems>

**Software Engineering Institute**

**Steps for Creating National CSIRTs**

The purpose of this document is to provide a high-level description of a Computer Security Incident Response Team (CSIRT), the problems and challenges facing these CSIRTs, and the benefits for developing such a team or response capability at a national level.

<https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=53062>

**Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability**

In this report, the authors provide insight that interested organizations and governments can use to develop a national incident management capability.

<https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9221>

**Other National CSIRT Resources**

This collection contains information that governments can use to develop a National Computer Security Incident Response Team (NatCSIRT).

<https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=505132>

**Other CSIRT Resources**

These resources help you create and maintain a CSIRT, staff and train CSIRTs, and describe common issues CSIRTs face. Also included is information governments can use to develop and manage National CSIRTs.

<https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=505118>

**Cybersecurity Center Development**

Critical to these incident response efforts are cybersecurity centers, which are teams of experts who mitigate threats by identifying, protecting, detecting, responding to, and recovering from incidents. These centers may take the form of computer security incident response teams (CSIRTs), security operations centers (SOCs), product security incident response teams (PSIRTs), CSIRTs of national responsibility, or other similar incident management teams. This international capacity building, information sharing, and global cyber workforce development are key efforts in the pursuance of U.S. objectives in cyberspace. The SEI prepares these cybersecurity center teams to effectively assess and manage cybersecurity incidents.

<https://sei.cmu.edu/our-work/cybersecurity-center-development/>

**Forum of Incident Response and Security Teams [various resources]**

FIRST brings together a variety of computer security incident response teams from government, commercial, and educational organizations. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large. Apart from the trust network that FIRST forms in the global incident response community, FIRST also provides value added services.

<https://www.first.org>

**FIRST CSIRT Services Framework**

The Computer Security Incident Response Team (CSIRT) Services Framework is a high-level document describing in a structured way a collection of cyber security services and associated functions that Computer Security Incident Response Teams and other teams providing incident management related services may provide. The framework is developed by recognized experts from the FIRST community with strong support from the Task Force CSIRT (TF-CSIRT) Community, and the International Telecommunications Union (ITU).

<https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1>

**National Institute of Standards and Technology (NIST)**

**Cybersecurity Framework:**

Helping organizations to better understand and improve their management of cybersecurity risk

* Main Site: <https://www.nist.gov/cyberframework>
* International Resources (including translations and adaptations): <https://www.nist.gov/cyberframework/international-resources>

**Privacy Framework:**

The NIST Privacy Framework is a voluntary tool developed in collaboration with stakeholders intended to help organizations identify and manage privacy risk to build innovative products and services while protecting individuals’ privacy

<https://www.nist.gov/privacy-framework>

**IoT Cybersecurity Program:**

NIST’s Cybersecurity for the Internet of Things (IoT) program supports the development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed. By collaborating with stakeholders across government, industry, international bodies, and academia, the program aims to cultivate trust and foster an environment that enables innovation on a global scale. Main site (includes links to published documents, documents out for comment, and upcoming workshops)

<https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program>

**National Initiative for Cybersecurity Education (NICE):**

The mission of NICE is to energize, promote, and coordinate a robust community working together to advance an integrated ecosystem of cybersecurity education, training, and workforce development.

* Main site: <https://www.nist.gov/itl/applied-cybersecurity/nice>
* NICE Framework: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf>

**National Cybersecurity Center of Excellence (NCCoE):**

Each project results in a freely available NIST Cybersecurity Practice Guide (Special Publication series 1800), which includes information and instructions organizations can use to implement an example solution for themselves. Organizations that want to adopt similar solutions can use products from our collaborating vendors, or products with similar characteristics that fit their budgets and IT infrastructure.

<https://www.nccoe.nist.gov>

**Small Business Cybersecurity Corner:**

Your resources for keeping your small business secure. Get cybersecurity basics, guidance, solutions, and training to protect your information and manage your cybersecurity risks.

<https://www.nist.gov/itl/smallbusinesscyber>

**Thailand Cybersecurity Act, English**

<https://thainetizen.org/wp-content/uploads/2019/11/thailand-cybersecrutiy-act-2019-en.pdf>