Florida Association Of County Attorneys 2020 Midyear Seminar

Protecting Sensitive Information & Mitigating Cyber Risk

PSA Kirby Wedekind
December 15, 2020

Agenda

- CISA Mission
- Best Practices
- Protected Critical Infrastructure Information
- Vulnerability Assessments

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient critical infrastructure for the American people.

MISSION

Lead the national effort to understand and manage cyber and physical risk to our critical infrastructure.

CORE COMPETENCIES

Partnership Development

CISA fosters collaborative partnerships that enable partners in the government and private sector to make informed, voluntary decisions and investments.

Every day, CISA employees: Share information with critical infrastructure partners and stakeholder and serve as the national hub for cybersecurity and communications information data sharing in near-real-time.

Sector outreach: CISA works with government officials and critical infrastructure stakeholders to plan, develop and facilitate exercises that build capacity, improve security and bolster resilience.

Threats to Critical Infrastructure

- America remains at risk from a variety of threats including:
  - Acts of Terrorism
  - Cyber Attacks
  - Extreme Weather
  - Pandemics
  - Accidents or Technical Failures

Best Practice: Backups

- Maintain offline, encrypted backups of data and to regularly test your backups
  - Backup procedures should be conducted on a regular basis.
  - Backups should be maintained offline as many ransomware variants attempt to find and delete any accessible backups.
  - Maintaining offline, current backups is most critical because there is no need to pay a ransom for data that is readily accessible to your organization.

Best Practice: Scan & Patch

- Conduct regular vulnerability scanning to identify and address vulnerabilities, especially those on internet-facing devices, to limit the attack surface.
  - CISA offers a no-cost Vulnerability Scanning service and other no-cost assessments: https://www.cisa.gov/cyber-resource-hub
- Regularly patch and update software and OSs to the latest available versions.
  - Prioritize timely patching of internet-facing servers—as well as software processing internet data, such as web browsers, browser plugins, and document readers—for known vulnerabilities.

Best Practice: Plan & Train

- Create, maintain, and exercise a basic cyber incident response plan and associated communications plan that includes response and notification procedures for a ransomware incident.
- Implement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity (e.g., phishing) or incidents. Conduct organization-wide phishing tests to gauge user awareness and reinforce the importance of identifying potentially malicious emails.

Protected Critical Infrastructure Information

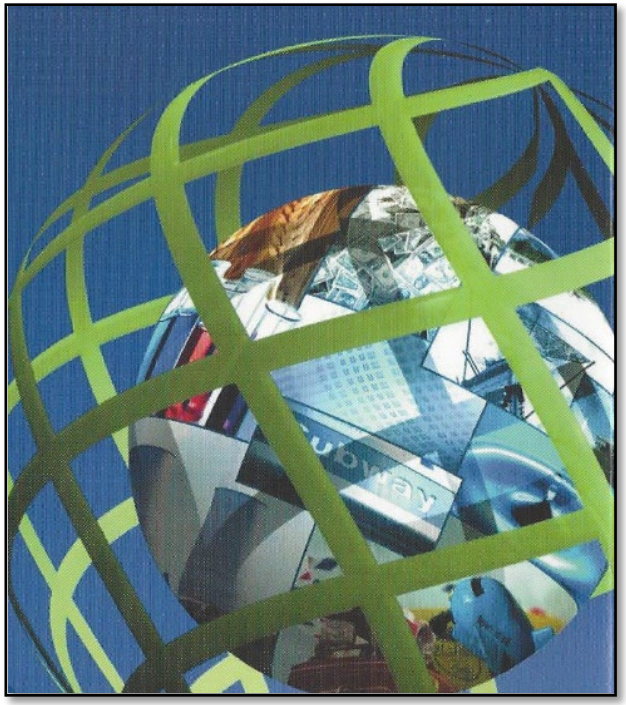
- The Protected Critical Infrastructure Information (PCII) Program protects critical infrastructure information voluntarily shared with the federal government for homeland security purposes
- PCII protects from release through:
  - Freedom of Information Act disclosure requests
  - State, local, tribal, territorial disclosure laws
  - Use in civil litigation
  - Use for regulatory purposes

Protected Critical Infrastructure Information

- Examples of organizations who submit information for PCII protections are:
  - Critical infrastructure owners and operators
  - State, local, tribal, territorial governments
  - Collaborative homeland security working groups

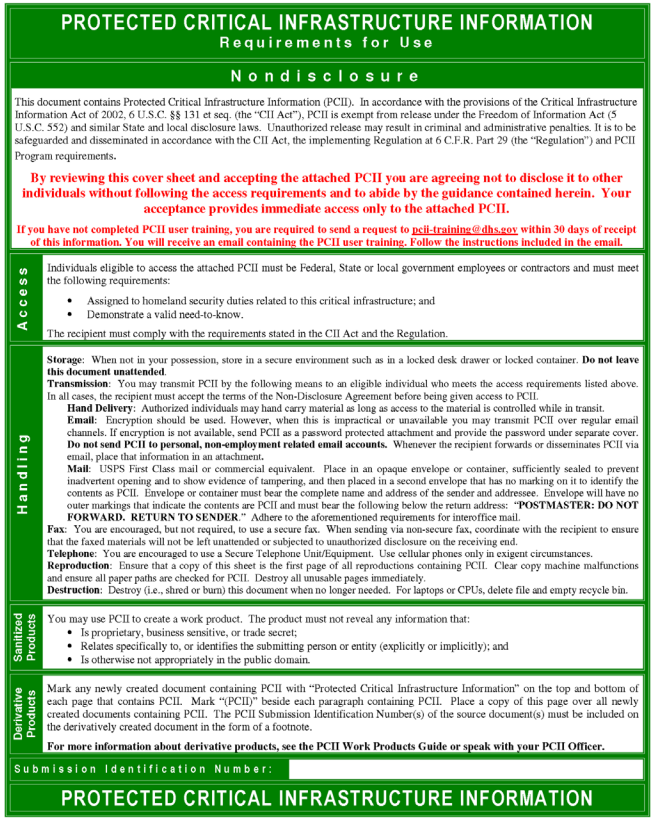
Protected Critical Infrastructure Information

- Allows CISA and other Federal, SLTT security analysts to use PCII to:
  - Analyze and secure critical infrastructure and protected systems (cyber)
  - Identify vulnerabilities and develop risk assessments
  - Enhance recovery preparedness measures



Protected Critical Infrastructure Information

- To qualify for PCII protections, information must be related to the security of the critical infrastructure and a submitter must attest the information is:
  - Voluntarily submitted
  - Not customarily found in the public domain
  - Not submitted in lieu of compliance with any regulatory requirement



PROTECTED CRITICAL INFRASTRUCTURE INFORMATION
Requirements for Use

Nondisclosure

This document contains Protected Critical Infrastructure Information (PCII). In accordance with the provisions of the Critical Infrastructure Information Act of 2002, 6 U.S.C. §§ 131 et seq. (the "CII Act"), PCII is exempt from release under the Freedom of Information Act (5 U.S.C. 552) and similar State and local disclosure laws. Unauthorized release may result in criminal and administrative penalties. It is to be safeguarded and disseminated in accordance with the CII Act, the implementing Regulation at 6 C.F.R. Part 29 (the "Regulation") and PCII Program requirements.

By reviewing this cover sheet and accepting the attached PCII you are agreeing not to disclose it to other individuals without following the access requirements and to abide by the guidance contained herein. Your acceptance provides immediate access only to the attached PCII.

If you have not completed PCII user training, you are required to send a request to pcii-training@dhs.gov within 30 days of receipt of this information. You will receive an email containing the PCII user training. Follow the instructions included in the email.

Access

Individuals eligible to access the attached PCII must be Federal, State or local government employees or contractors and must meet the following requirements:

- Assigned to homeland security duties related to this critical infrastructure; and
- Demonstrate a valid need-to-know.

The recipient must comply with the requirements stated in the CII Act and the Regulation.

Handling

Storage: When not in your possession, store in a secure environment such as in a locked desk drawer or locked container. **Do not leave this document unattended.**

Transmission: You may transmit PCII by the following means to an eligible individual who meets the access requirements listed above. In all cases, the recipient must accept the terms of the Non-Disclosure Agreement before being given access to PCII.

Hand Delivery: Authorized individuals may hand carry material as long as access to the material is controlled while in transit.

Email: Encryption should be used. However, when this is impractical or unavailable you may transmit PCII over regular email channels. If encryption is not available, send PCII as a password protected attachment and provide the password under separate cover. **Do not send PCII to personal, non-employment related email accounts.** Whenever the recipient forwards or disseminates PCII via email, place that information in an attachment.

Mail: USPS First Class mail or commercial equivalent. Place in an opaque envelope or container, sufficiently sealed to prevent inadvertent opening and to show evidence of tampering, and then placed in a second envelope that has no marking on it to identify the contents as PCII. Envelope or container must bear the complete name and address of the sender and addressee. Envelope will have no outer markings that indicate the contents are PCII and must bear the following below the return address: "**POSTMASTER: DO NOT FORWARD. RETURN TO SENDER.**" Adhere to the aforementioned requirements for interoffice mail.

Fax: You are encouraged, but not required, to use a secure fax. When sending via non-secure fax, coordinate with the recipient to ensure that the faxed materials will not be left unattended or subjected to unauthorized disclosure on the receiving end.

Telephone: You are encouraged to use a Secure Telephone Unit/Equipment. Use cellular phones only in exigent circumstances.

Reproduction: Ensure that a copy of this sheet is the first page of all reproductions containing PCII. Clear copy machine malfunctions and ensure all paper paths are checked for PCII. Destroy all unusable pages immediately.

Destruction: Destroy (i.e., shred or burn) this document when no longer needed. For laptops or CPUs, delete file and empty recycle bin.

Sanitized Products

You may use PCII to create a work product. The product must not reveal any information that:

- Is proprietary, business sensitive, or trade secret;
- Relates specifically to, or identifies the submitting person or entity (explicitly or implicitly); and
- Is otherwise not appropriately in the public domain.

Derivative Products

Mark any newly created document containing PCII with "Protected Critical Infrastructure Information" on the top and bottom of each page that contains PCII. Mark "(PCII)" beside each paragraph containing PCII. Place a copy of this page over all newly created documents containing PCII. The PCII Submission Identification Number(s) of the source document(s) must be included on the derivatively created document in the form of a footnote.

For more information about derivative products, see the PCII Work Products Guide or speak with your PCII Officer.

Submission Identification Number:

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

Protected Critical Infrastructure Information

- To become a PCII Authorized User (AU), one must:
  - Be a government employee or supporting contractor
  - Have specific homeland security duties
  - Have a specific “Need-to-Know”
  - Complete PCII Authorized User training
  - Sign a Non-Disclosure Agreement (except Federal employees)
- PCII protects oral discussions
- PCII can be emailed on government systems
- PCII can be stored electronically on approved Government systems
- PCII can be stored in controlled spaces in locked containers (GSA safe NOT required)

Protected Critical Infrastructure Information

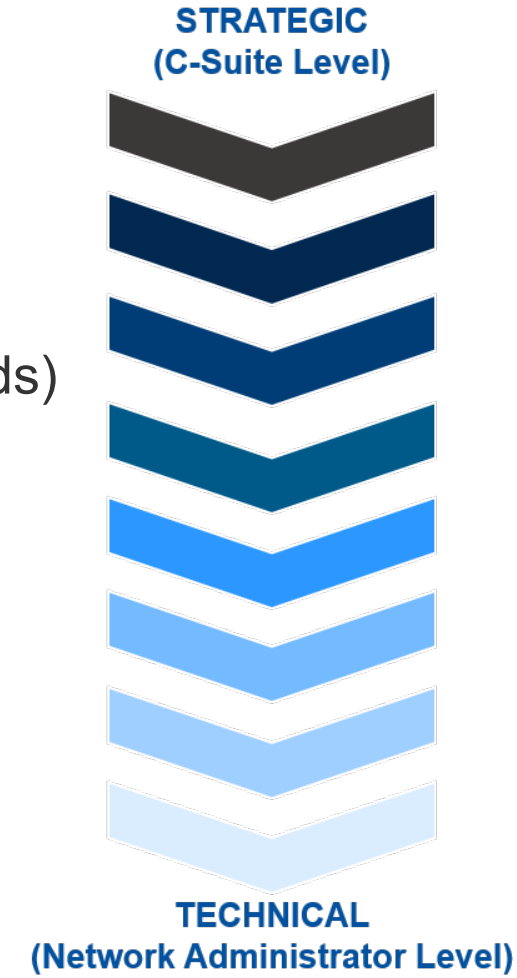
- ***PCII is too difficult to share!"***
  - Sanitize the information if possible
  - Share with PCII Authorized Users using derivative products
  - PCII Authorized Users can email PCII with minimal actions on unclassified government networks
  - Exigent circumstances
- "***Marking and handling PCII is like classified information"***
  - PCII is Sensitive But Unclassified (SBU)
  - Can be accessed on UNCLASS network and shared with PCII Authorized Users
- ***"Other protections exist to prevent disclosure/release"***
  - PCII has a specific statutory exemption (CII Act of 2002) from release

Cybersecurity Advisor Program

- Cybersecurity Advisors (CSA) offer assistance to help prepare and protect private sector entities and governments from cybersecurity threats
  - **Assess:** Evaluate critical infrastructure cyber risk
  - **Promote:** Encourage best practices and risk mitigation strategies
  - **Build:** Initiate, develop capacity, and support cyber communities-of-interest and working groups
  - **Educate:** Inform and raise awareness
  - **Listen:** Collect stakeholder requirements
  - **Coordinate:** Bring together incident support and lessons learned

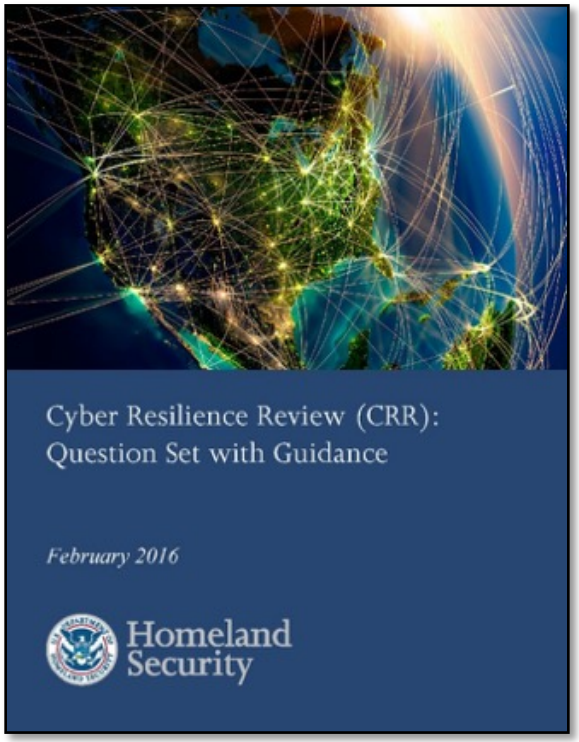
Cybersecurity Assessments

- Cyber Resilience Review (Strategic)
- External Dependencies Management (Strategic)
- Cyber Infrastructure Survey (Strategic)
- Cybersecurity Evaluations Tool Strategic (Standards)
- Phishing Campaign Assessment (EVERYONE)
- Validated Architecture Design Review (Technical)
- Vulnerability Scanning / Hygiene (Technical)
- Remote Penetration Test (Technical)
- Risk and Vulnerability Assessment (Technical)



Cyber Resiliency Review

- Evaluates operational resilience and cybersecurity practices of critical services.
- CSA-facilitated or self-administered
- Helps public and private sector partners understand and measure cybersecurity capabilities as they relate to operational resilience and cyber risk



External Dependencies Management Assessment

- Provides an organization with a better understanding of how they manage risks arising from dependences on the information and communication technology supply chain.

- Focuses on Information and Communication Technology Supply Chain Risk Management (ICT SCRM)

Vulnerability Scanning

- Imagining your organization's information network as a house,
- Vulnerability scans show you **the digital equivalent of:**

1. How big your house is
2. Which doors and windows are locked or not
3. Which blinds and curtains are closed or what is visible if they're open
4. General maintenance (i.e. mowed lawn, new roof, curb appeal)

For more information:
cisa.gov

Questions?
Kirby.Wedekind@HQ.DHS.GOV
(202) 868-1361


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY

Information and Communications Supply Chain Risk Management

- Protecting your organization's information in a digitally-connected world requires understanding not only your organization's immediate supply chain, but also the extended supply chains of third-party vendors, service providers, and customers. These essential steps will assist your organization in managing supply chain risks and building an effective SCRM practice.
  - **Identify** the people: Build a cross-functional team of representatives from across the organization (e.g., cybersecurity, information technology, physical security, procurement/acquisition, legal, logistics, marketing, and product development).
  - **Manage** the security and compliance: Document the set of policies and procedures that address security, integrity, resilience, and quality. Ensure they are based on industry standards and best practices on how to conduct SCRM such as those from the National Institute of Standards and Technology (NIST).
  - **Assess** the components: Build a list of ICT components (e.g., hardware, software, and services) that your organization procures to enable your business. Know which internal systems are relied upon for critical information or functions, and which systems have remote access capability that must be protected to prevent unauthorized access.

Information and Communications Supply Chain Risk Management

- Protecting your organization's information in a digitally-connected world requires understanding not only your organization's immediate supply chain, but also the extended supply chains of third-party vendors, service providers, and customers. These essential steps will assist your organization in managing supply chain risks and building an effective SCRM practice.
  - **Know** the supply chain and suppliers: Identify your suppliers and, when possible, the suppliers' sources. In today's world of increased outsourcing, it is important to understand your upstream suppliers as part of the larger supply chain ecosystem.
  - **Verify** assurance of third-parties: Verify that your suppliers maintain an adequate security culture and SCRM program to appropriately address the risks that concern your organization. Establish the protocols your organization will use to assess the supply chain practices of your suppliers.
  - **Evaluate** your SCRM program: Determine the frequency with which to review your SCRM program, incorporate feedback, and make changes to your risk management program. This may also include auditing suppliers against practices and protocols established by your organization.