CISA SECURITY ASSESSMENTS FOR HOSPITALS

Pete Owen
December 1, 2023

Purpose & outline

The purpose of this presentation is to inform members of the Central New York Hospital Emergency Preparedness Coalition about the security assessments the Cybersecurity and Infrastructure Security Agency can perform.

Outline

- Who we are
- Assessments
- Other ways we can help

Who we are

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient infrastructure for the American public

MISSION

CISA partners with industry and government to understand and manage risk to our Nation's critical infrastructure.

OVERALL GOALS

GOAL 1

DEFEND TODAY

Defend against urgent threats and hazards

seconds | days | weeks

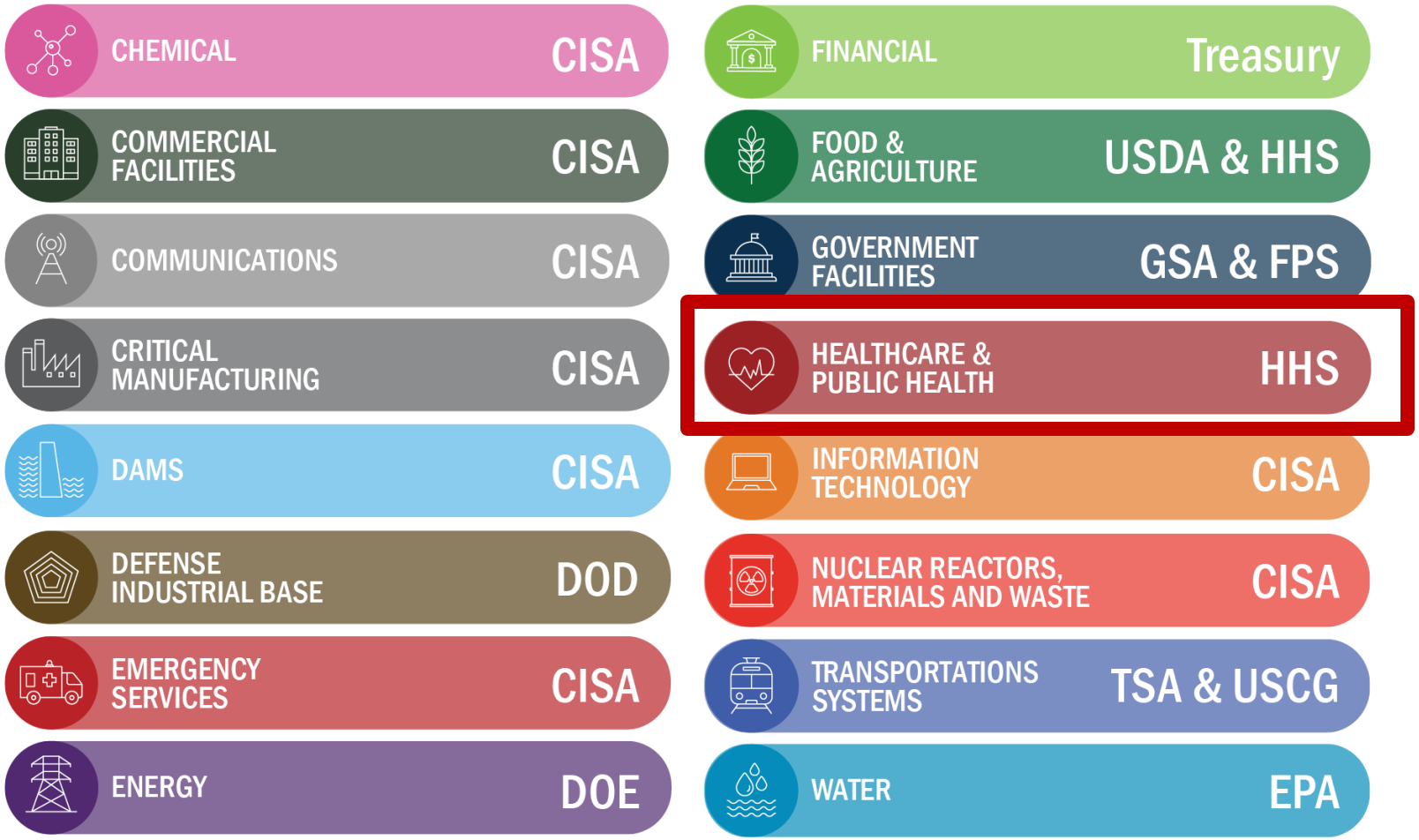
GOAL 2

SECURE TOMORROW

Strengthen critical infrastructure and address long-term risks

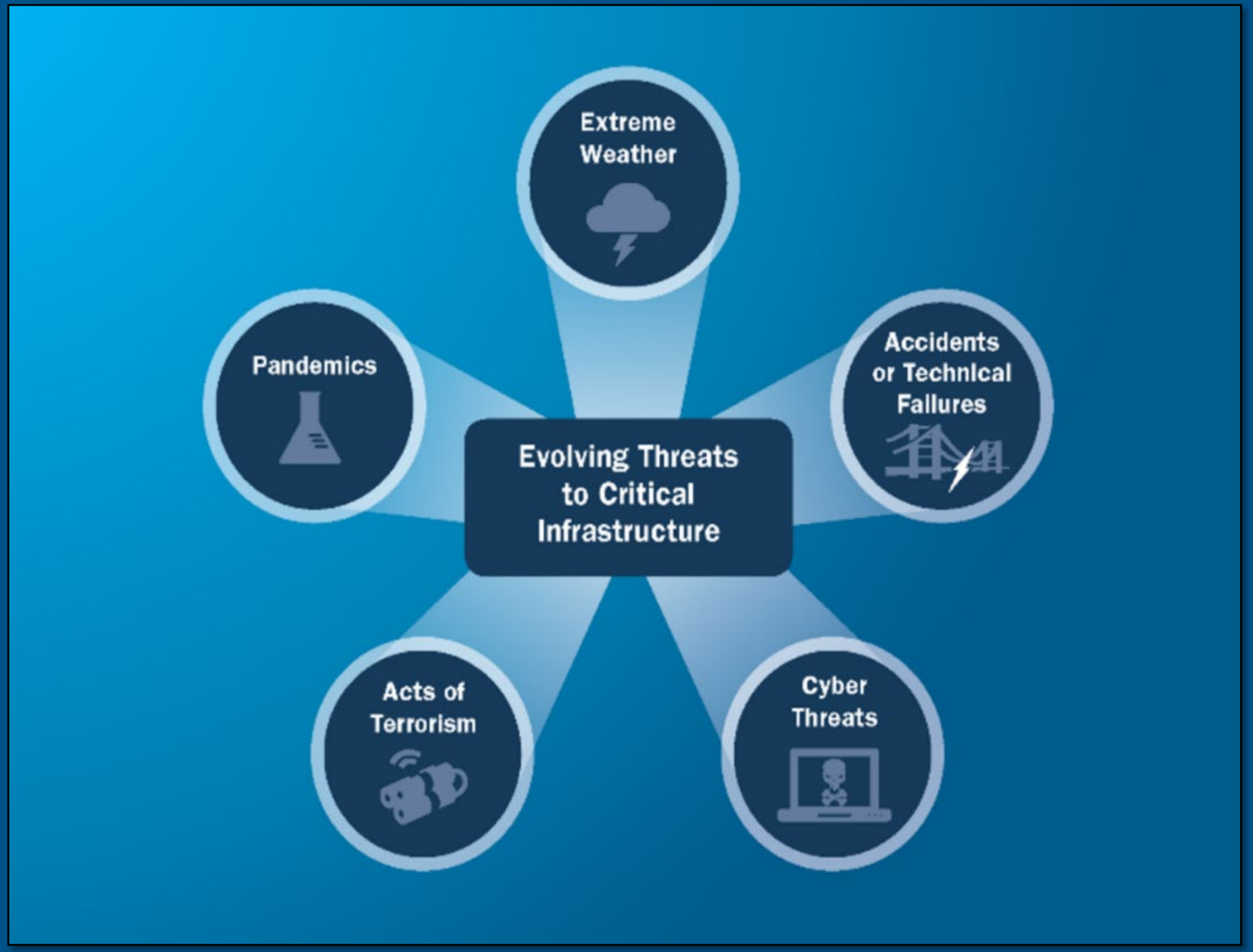
months | years | decades

16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies



Threats

- Criminals
- Sabotage
- Espionage

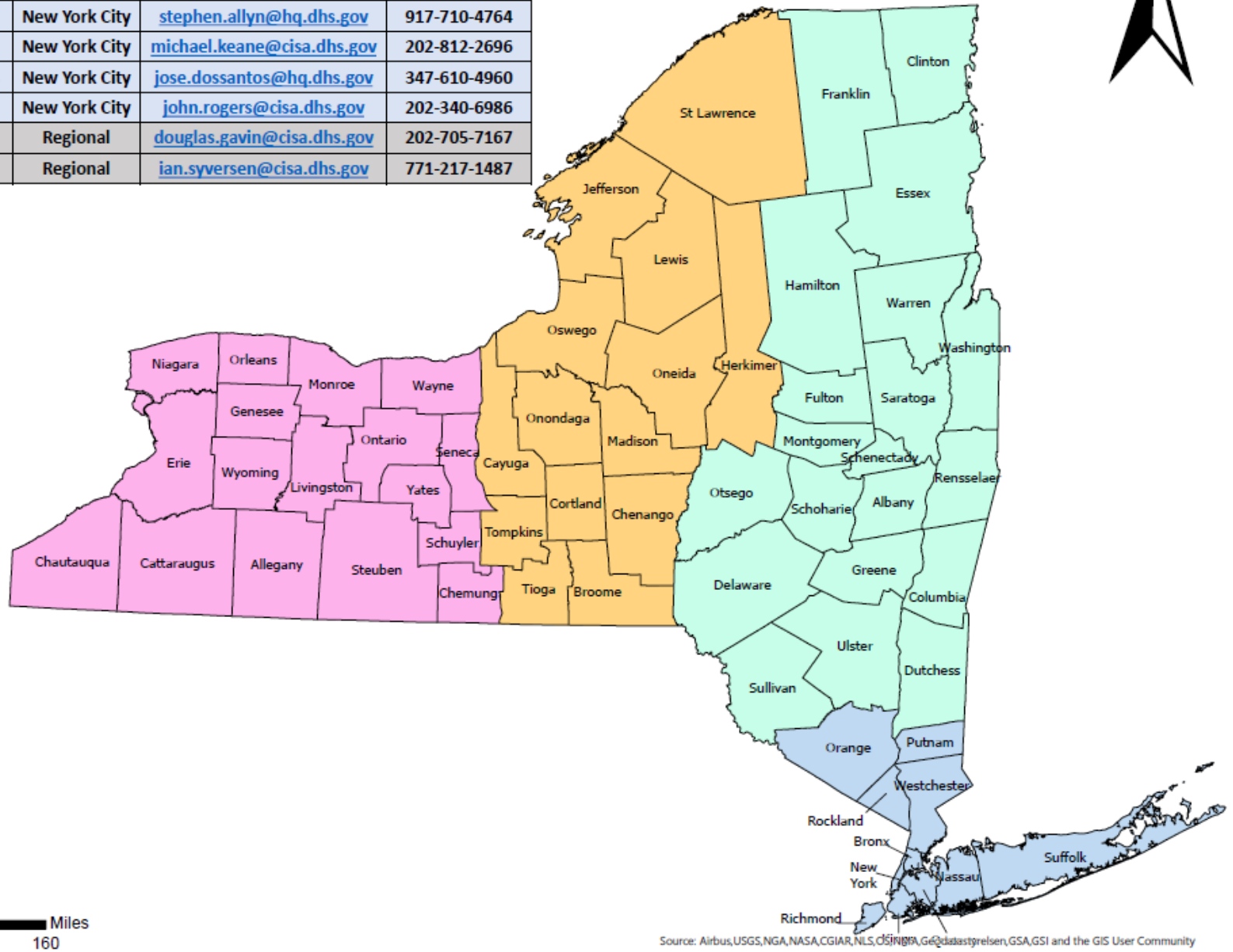


Protective Security Advisors

Five mission areas:

- Security assessments
- Share information
- Security of soft targets and crowded places
- Bombing prevention and other training
- Special events and domestic incident support

Region II Position Title	Name	District	Email	Phone
Protective Security Advisor	TBD	Buffalo	TBD	TBD
Protective Security Advisor Lead	Peter Owen	Syracuse	peter.owen@hq.dhs.gov	619-733-9262
Protective Security Advisor	James Marcello	Albany	james.marcello@hq.dhs.gov	202-852-2055
Protective Security Advisor	Stephen Allyn	New York City	stephen.allyn@hq.dhs.gov	917-710-4764
Protective Security Advisor	Michael Keane	New York City	michael.keane@cisa.dhs.gov	202-812-2696
Protective Security Advisor	Jose DosSantos	New York City	jose.dossantos@hq.dhs.gov	347-610-4960
Protective Security Advisor	John Rogers	New York City	john.rogers@cisa.dhs.gov	202-340-6986
Regional Protective Security Advisor	Douglas Gavin	Regional	douglas.gavin@cisa.dhs.gov	202-705-7167
Chief of Protective Security	Ian Syversen	Regional	ian.syversen@cisa.dhs.gov	771-217-1487



Security assessments

Overview

- The Cybersecurity and Infrastructure Security Agency (CISA) conducts assessments of physical security and resilience on critical infrastructure facilities.
- Assessments are free.
- Assessments are voluntary.
- Information is protected from disclosure by federal law.
- The tool CISA uses is called the Infrastructure Survey Tool, or “IST.”

Protected Critical Infrastructure Information

PCII protects info from release from:

- Freedom of Information Act requests
- State, local, tribal, territorial disclosure laws
- Use in civil litigation
- Use for regulatory purposes

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:

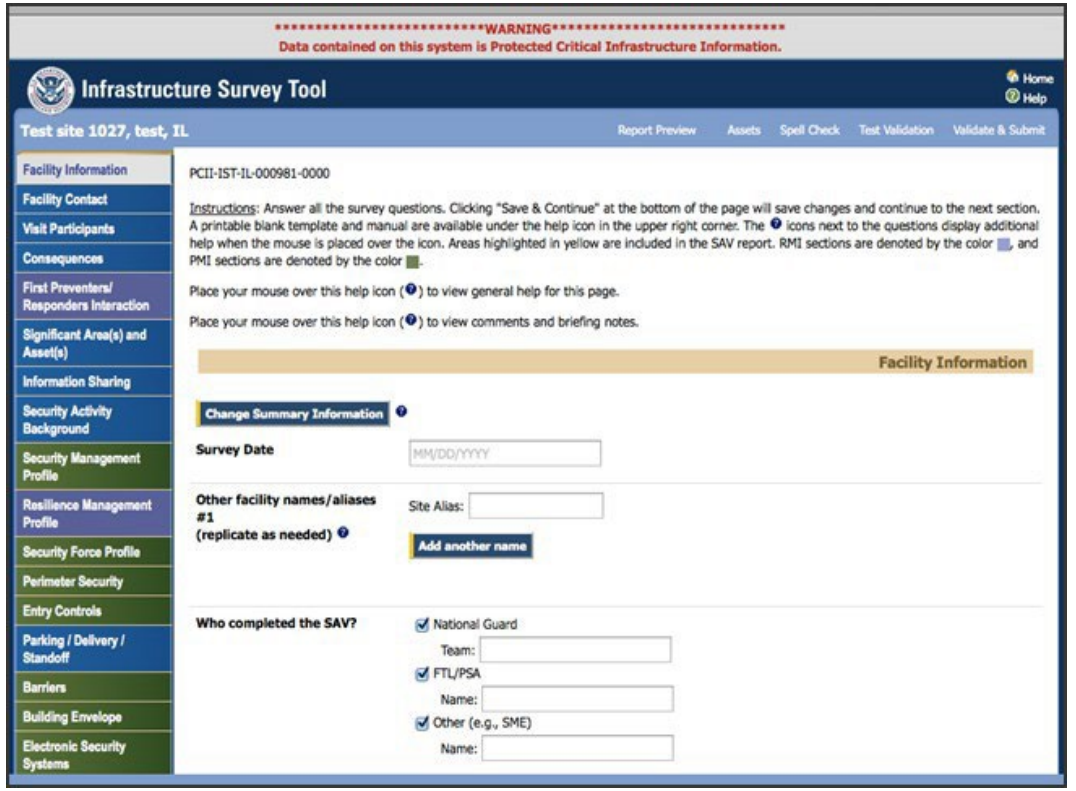
PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

Security surveys and assessments

- Detailed assessments of critical infrastructure (one day)
- Security walk throughs for smaller buildings (1-2 hours)
- 360-degree video captures of critical infrastructure (1-2 days)
- Mass gathering assessments (1-2 hours)

Infrastructure Survey Tool ("IST")

- A web-based security survey
- Applies weighted scores to vulnerabilities
- Consistent, objective assessment
  - Physical Security
  - Security Force
  - Security Management
  - Information Sharing
  - Protective Measures
  - Dependencies



Pete Owen
December 1, 2023

Conduct of the survey (6-8 hours)

- Introductions and overview
- Walk through
- Interviews with key folks such as
  - Security manager
  - Facility manager
  - Operations manager
  - Emergency and business continuity planner(s)
  - IT security
  - Human resources
- Out brief
- Report delivery 30-45 days later

Pete Owen
December 1, 2023

Survey Components

Physical Security (212)

- Fences (26)
- Gates (54)
- CCTV (6)
- IDS (39)
- Parking (10)
- Access Control (44)
- Security Lighting (15)
- Vehicle Access Control (9)
- Building Envelope (9)

Security Management (43)

- Business continuity plan
- Security plan
- Emergency Action Plan
- Threat Levels
- Security Info. Communication
- External Security Exercises
- Executive protection program
- Security working groups
- Sensitive information identified
- National Security Clearance
- Background Checks

Security Force (59)

- Staffing
- Equipment/Weapons
- Training
- Post guidelines
- Patrols
- Random Patrols
- After hour security
- Checks recorded
- Command and control
- MOU/MOA

Information Sharing (22)

- Threat Sources
- Information Sharing Mechanisms

Protective Measures (23)

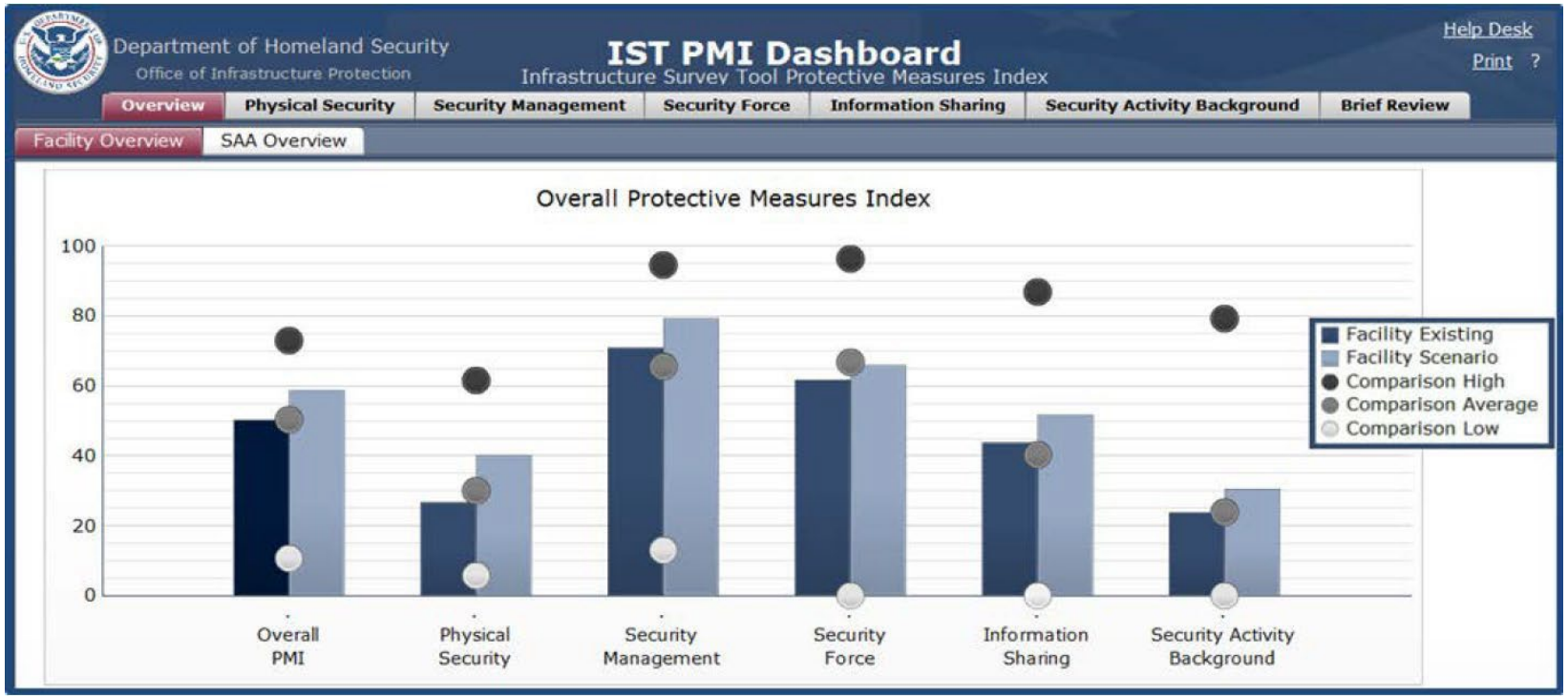
- New Protective Measures
- Random Security Measures

Dependencies (216)

- Critical Products (42)
- Electric (23)
- Information Technology (58)
- Natural Gas (12)
- Telecommunications (32)
- Transportation (20)
- Water (14)
- Wastewater (15)

Two-part report

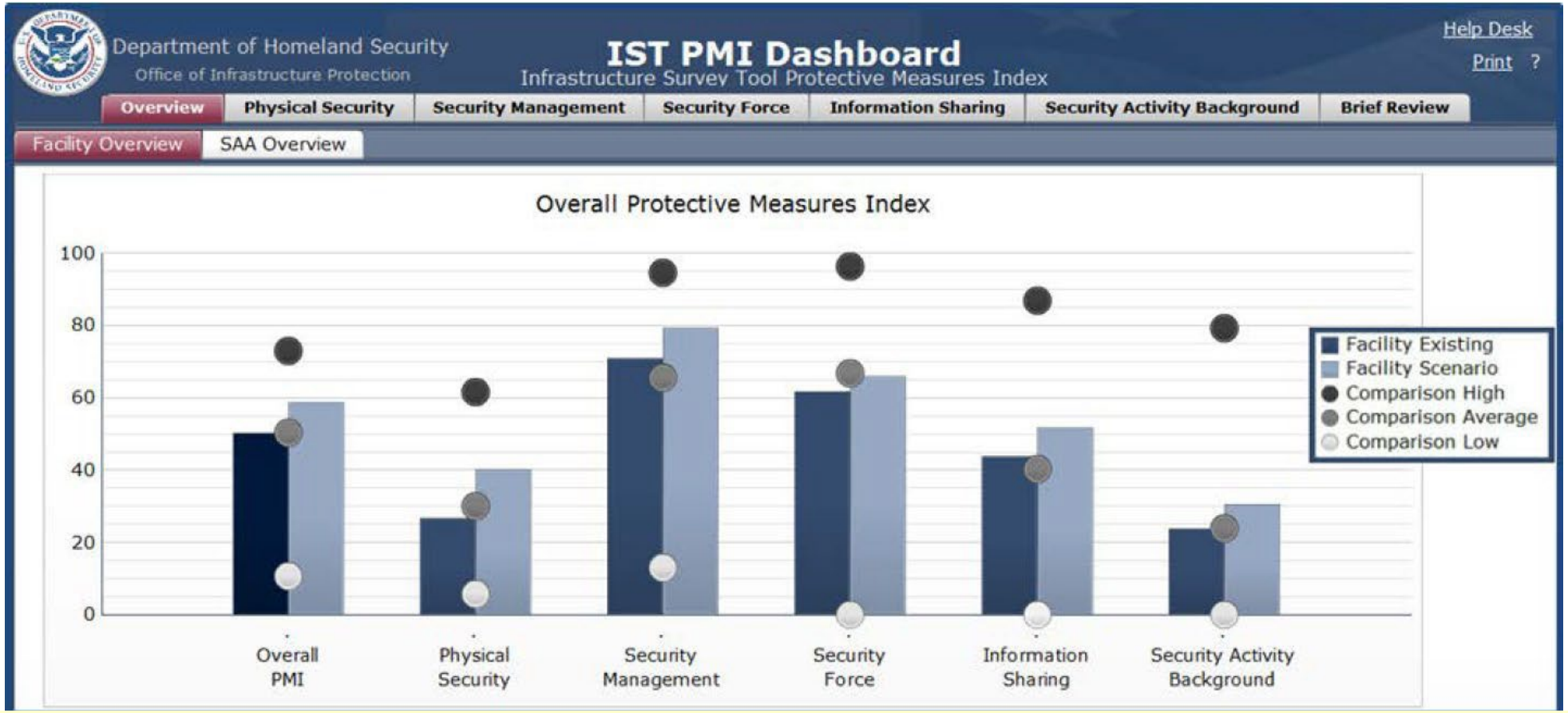
The interactive dashboard compares the results of the survey to data collected and similar facilities.



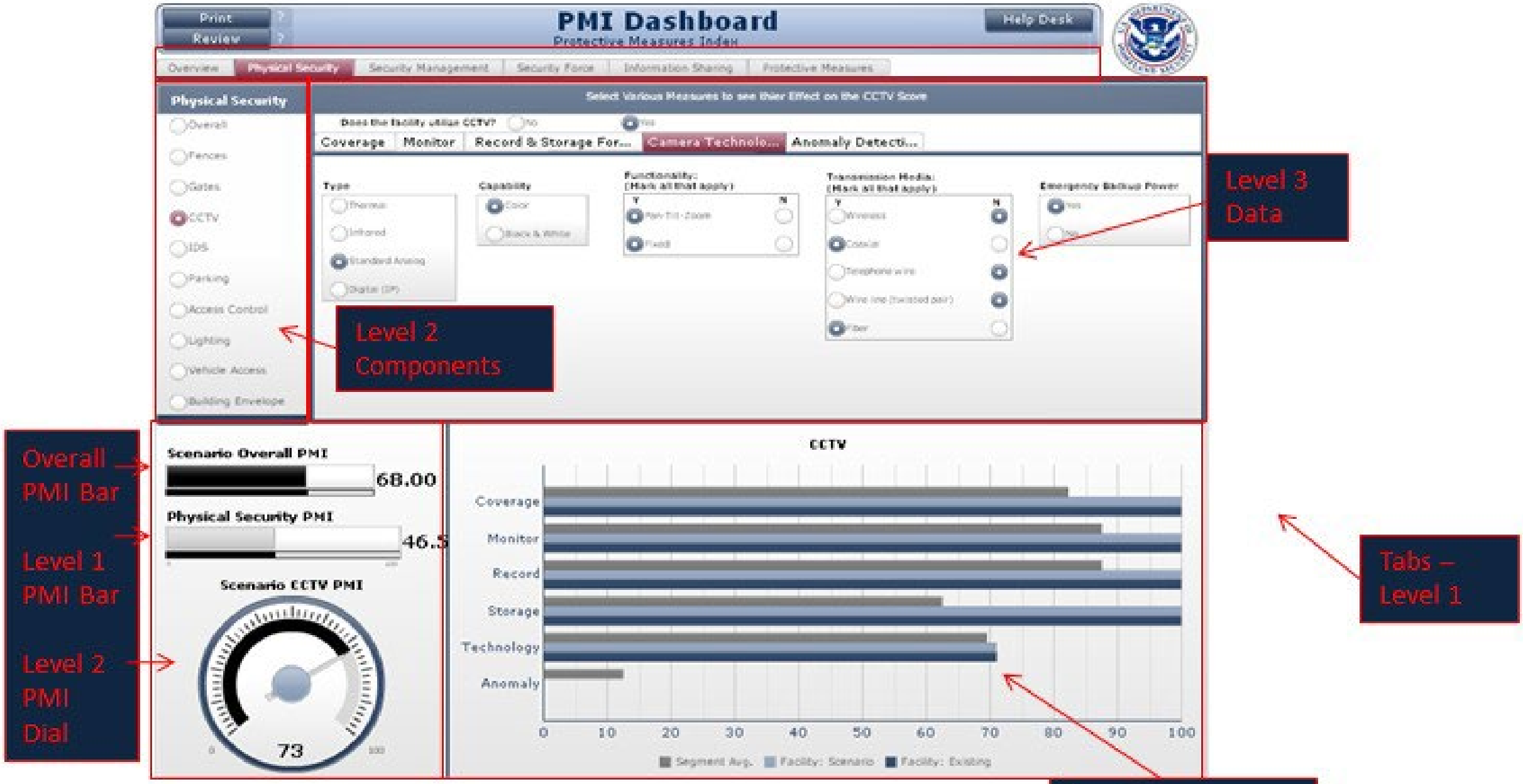
The written report describes the facility, identifies its vulnerabilities, and provides options to mitigate each vulnerability.

Pete Owen
December 1, 2023

Dashboard report



This example shows a facility's Protective Measures Index (PMI) and compares its scores (the blue bars) to the sector averages (the gray dots).



This example shows a facility's survey responses for CCTV and compares its score (in blue) to the sector average (in grey).

Dashboard Weighting and Scoring

- Weighting and scoring was developed by a working group comprised of:
  - Physical security experts
  - Scientists
  - Mathematicians
  - Sector representatives
  - Owners and operators of facilities being weighted
- Weights validated using a separate panel of representatives
- Example: Fence Protective Measures Index (PMI)

- Aluminum chain link fence
- 7 feet high
- Clear zone
- Barbed wire outriggers
- Fence PMI = 71

- Wood fence
- 6 feet high
- Partial clear zone
- Fence PMI = 13

Pete Owen
December 1, 2023

SAFE Tool

- The Security Assessment at First Entry (SAFE) tool is designed to assess the current security posture and identify options for facility owners and operators to mitigate relevant threats
- The SAFE tool is suited for all facilities, including smaller ones such as museums, small businesses, and health clinics.

Other ways we can help

Active Shooter Preparedness

- "How to Respond" resource materials
- Preparedness videos and training links
- Emergency action planning tools and templates

https://www.cisa.gov/active-shooter-preparedness

Active Shooter Preparedness Training

- Videos
- Independent study online
- In person
  - Run. Hide. Fight.®
  - Organizational preparedness
- Online workshops
- Exercises

“Options for Consideration” video

https://youtu.be/i3QBktsRKVY?si=pTyXIEGuHuxtIWWR

Active Shooter Online Courses

IS-904: Active Shooter Prevention:
You Can Make a Difference

- Recognize indicators and concerning behaviors
- Empathy and compassion techniques to reduce the likelihood an event will escalate
- Identify situations where professional help could be used
- Traits of a connected, supportive work environment

https://training.fema.gov/is/courseoverview.aspx?code=IS-904&lang=en

IS-907: Active Shooter:
What You Can Do

- Actions to take when confronted with an active shooter (Run. Hide. Fight.®)
- Recognize workplace violence indicators
- Actions to take to prevent and prepare for potential active shooter incidents.
- How to manage the consequences of an active shooter incident

https://training.fema.gov/is/courseoverview.aspx?code=is-907&lang=en

Active Shooter Preparedness Workshops

- Scenario-based workshops to help participants prepare for active shooter emergencies
- Participants evaluate response concepts, plans, and capabilities in guided discussions
- Active Shooter Preparedness Webinar
  - Tuesday, 30 January 2024, 1:00 – 3:00 PM EST
- Active Shooter Preparedness Workshop, in-person in Buffalo
  - Friday, 16 February 2024, at 8:00 AM to 4:00 PM EST

https://www.cisa.gov/active-shooter-workshop-participant

Managing Bomb Threats

What to Do - Bomb Threat | CISA

- Training video
- Checklist
- Guidance

https://www.cisa.gov/bomb-threats

Suspicious Items

www.cisa.gov/resources-tools/resources/unattended-vs-suspicious-item-postcard-and-poster

https://about.usps.com/postal-bulletin/2019/pb22529/html/info_002.htm

Bombing Prevention Training

In-Person

- Bombing Prevention Awareness
- Bomb Threat Management Planning
- IED Search Procedures
- Protective Measures
- Surveillance Detection
- Vehicle-Borne Improvised Explosive Device Detection
- BMAP Community Liaisons

Virtual Instructor

- IED Construction and Classification
- IED Explosive Effects Mitigation
- Introduction to the Terrorist Attack Cycle
- Homemade Explosives and Precursor Awareness
- Protective Measures Awareness
- Response to Suspicious Behaviors and Items

Self-paced ISTs

- IED Awareness and Safety
- Homemade Explosives and Precursor Chemicals Awareness Bomb Threat Preparedness and Response
- Bomb-Making Materials Awareness: Your Role
- Bomb-Making Materials Awareness Employee Training

What To Do Training Videos

- Bomb Threat
- Bomb Searches
- Surviving a Bombing Attack
- Suspicious or Unattended Item

www.cisa.gov/bombing-prevention-training-courses

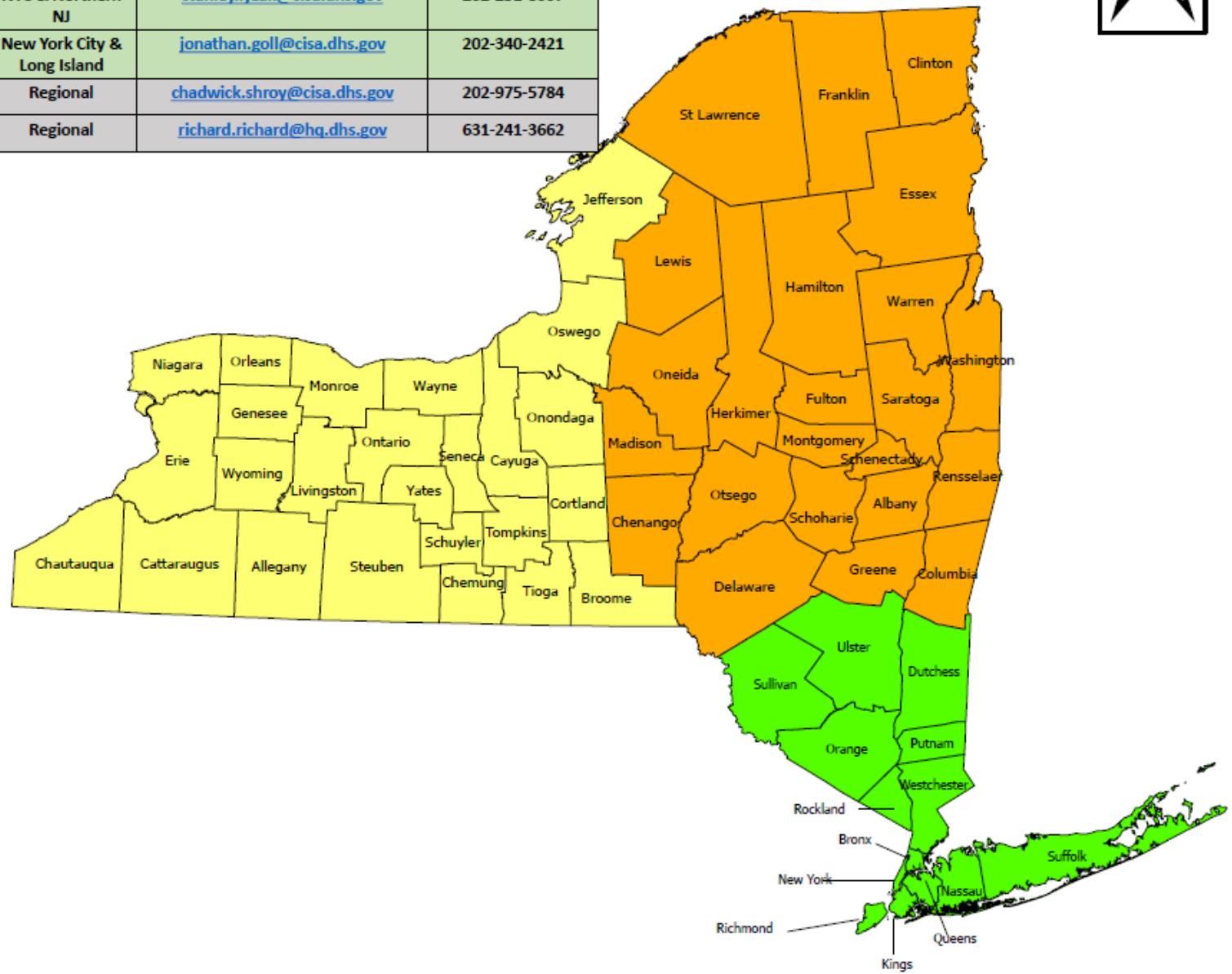
Cyber Security Resources

- Cyber Security Advisors
- Vulnerability Scanning
- Cybersecurity Evaluation Tool

Cyber Security Advisors

- 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.

Region II Position Title	Name	District	Email	Phone
Cybersecurity Advisor	Scott Patronik	Western NY	scott.patronik@cisa.dhs.gov	202-740-8095
Cybersecurity Advisor	Crystal Wilson	Albany & Northern NY	crystal.wilson@cisa.dhs.gov	202-445-4290
Cybersecurity Advisor	Jonathan Easton	NYC and Hudson Valley	jonathan.easton@cisa.dhs.gov	771-217-0640
Cybersecurity Advisor	Stanley Lyzak	NYC & Northern NJ	stanley.lyzak@cisa.dhs.gov	202-251-8337
Cybersecurity Advisor	Jonathan Goll	New York City & Long Island	jonathan.goll@cisa.dhs.gov	202-340-2421
Cybersecurity Advisor/Law Enforcement Liaison	Chadwick Shroy	Regional	chadwick.shroy@cisa.dhs.gov	202-975-5784
Chief of Cybersecurity	Richard Richard	Regional	richard.richard@hq.dhs.gov	631-241-3662



Legend

- Western NY
- Albany & Northern NY
- NYC & Hudson Valley

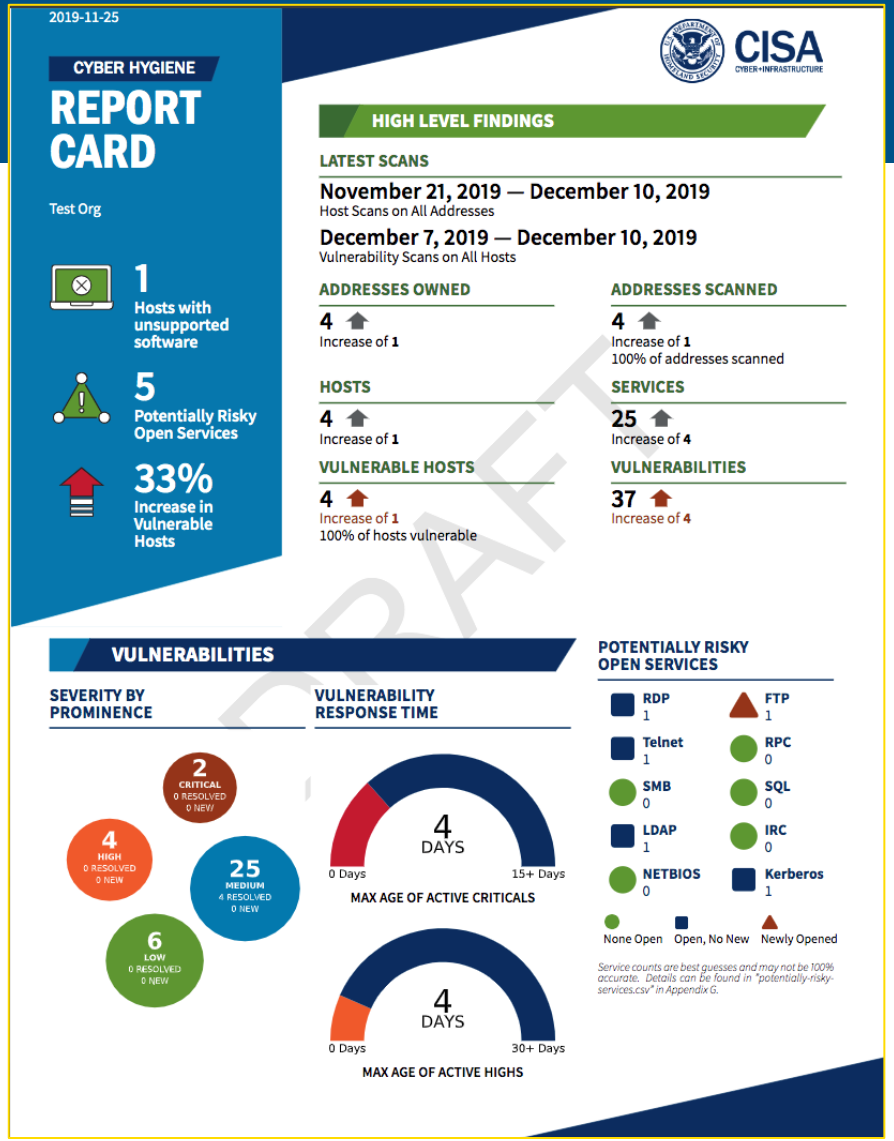
Cybersecurity Evaluation Tool

- Assesses control system and information system security against industry standards
- Self-Administered, undertaken independently
- Benefits:
  - Immediately available for download
  - Standards based
  - Ability to drill down on specific areas and issues

https://www.cisa.gov/downloading-and-installing-cset

Vulnerability Scanning

- Identify vulnerabilities directly accessible for exploitation via the Internet
- Continuous scanning with weekly reports and critical alerts
  - Internet-accessible vulnerabilities
  - Potentially risky services
  - Unsupported software



https://www.cisa.gov/resources-tools/services/cisa-vulnerability-scanning

Ready Business

Guides, training, and templates to help businesses develop and implement

- Emergency response plans
- Business continuity plans

www.ready.gov

For more information:

cisa.gov

Questions?

Email: peter.owen@hq.dhs.gov

Phone: (619) 733-9262