

CISA SECURITY ASSESSMENTS FOR HOSPITALS



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



Pete Owen
December 1, 2023

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

| | | | |
|--|------|--|------------|
|  CHEMICAL | CISA |  FINANCIAL | Treasury |
|  COMMERCIAL FACILITIES | CISA |  FOOD & AGRICULTURE | USDA & HHS |
|  COMMUNICATIONS | CISA |  GOVERNMENT FACILITIES | GSA & FPS |
|  CRITICAL MANUFACTURING | CISA |  HEALTHCARE & PUBLIC HEALTH | HHS |
|  DAMS | CISA |  INFORMATION TECHNOLOGY | CISA |
|  DEFENSE INDUSTRIAL BASE | DOD |  NUCLEAR REACTORS, MATERIALS AND WASTE | CISA |
|  EMERGENCY SERVICES | CISA |  TRANSPORTATIONS SYSTEMS | TSA & USCG |
|  ENERGY | DOE |  WATER | EPA |

Threats

Criminals

Sabotage

Espionage



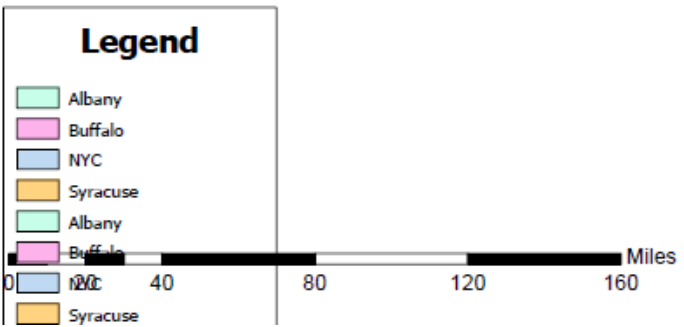
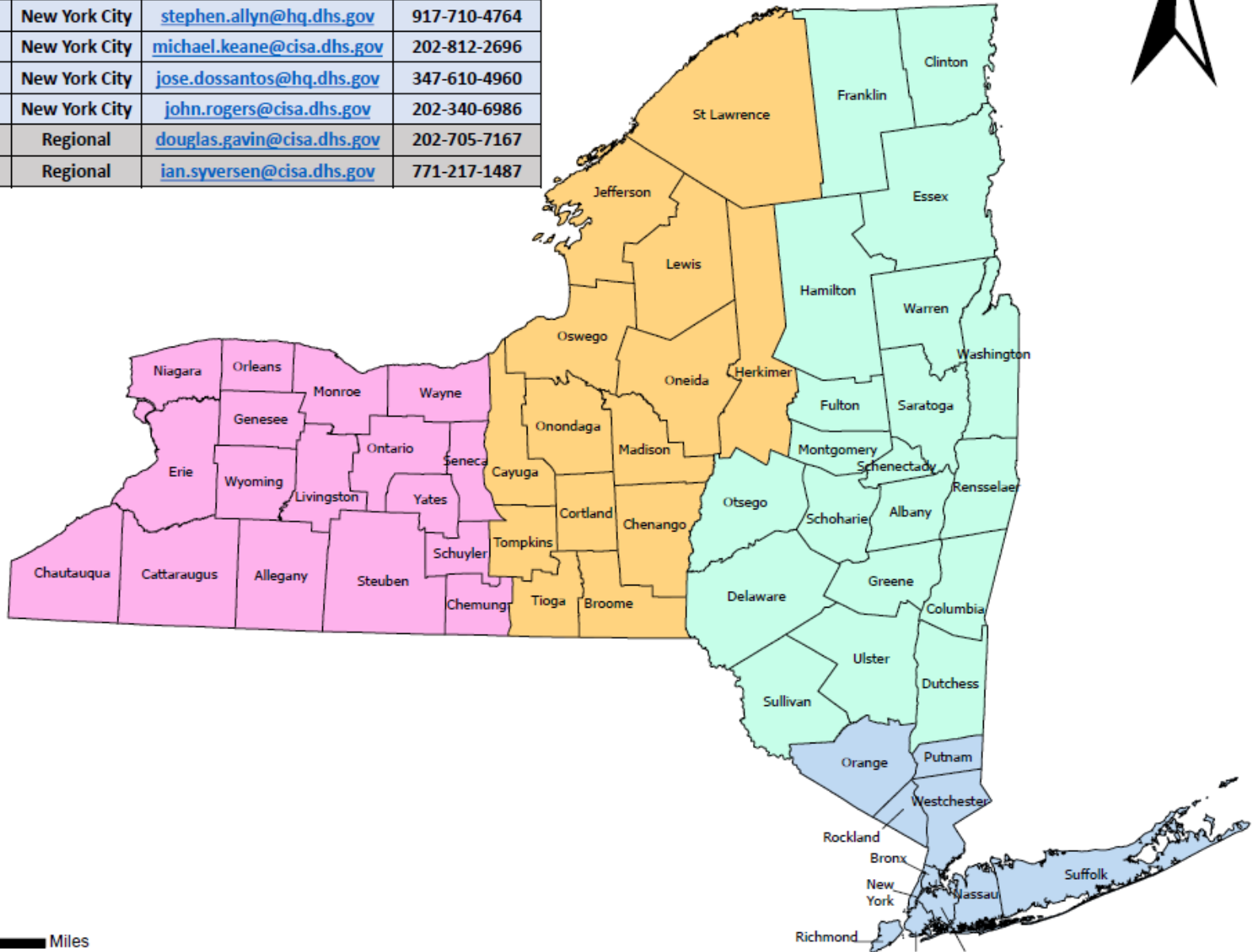
Protective Security Advisors

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 |



Source: Airbus,USGS,NGA,NASA,CGIAR,NLS,OSINT,GeoIntelligence,OpenStreetMap,GeoIntelligence,GSA,GSI and the GIS User Community

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 | |
| <p>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.</p> <p>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.</p> <p>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.</p> | |
| Access | <p>Individuals eligible to access the attached PCII must be Federal, State or local government employees or contractors and must meet the following requirements:</p> <ul style="list-style-type: none">• Assigned to homeland security duties related to this critical infrastructure; and• Demonstrate a valid need-to-know. <p>The recipient must comply with the requirements stated in the CII Act and the Regulation.</p> |
| Handling | <p>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.</p> <p>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.</p> <p>Hand Delivery: Authorized individuals may hand carry material as long as access to the material is controlled while in transit.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Telephone: You are encouraged to use a Secure Telephone Unit/Equipment. Use cellular phones only in exigent circumstances.</p> <p>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.</p> <p> Destruction: Destroy (i.e., shred or burn) this document when no longer needed. For laptops or CPUs, delete file and empty recycle bin.</p> |
| Sanitized Products | <p>You may use PCII to create a work product. The product must not reveal any information that:</p> <ul style="list-style-type: none">• 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 | <p>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.</p> <p>For more information about derivative products, see the PCII Work Products Guide or speak with your PCII Officer.</p> |
| Submission Identification Number: <input type="text"/> | |
| 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

*****WARNING*****
Data contained on this system is Protected Critical Infrastructure Information.

Infrastructure Survey Tool

Test site 1027, test, IL

PCII-IST-IL-000981-0000

Instructions: Answer all the survey questions. Clicking "Save & Continue" at the bottom of the page will save changes and continue to the next section. A printable blank template and manual are available under the help icon in the upper right corner. The icons next to the questions display additional help when the mouse is placed over the icon. Areas highlighted in yellow are included in the SAV report. RMI sections are denoted by the color .

Place your mouse over this help icon to view general help for this page.

Place your mouse over this help icon to view comments and briefing notes.

Facility Information

Change Summary Information

Survey Date

Other facility names/aliases #1 (replicate as needed)

Site Alias:

Add another name

Who completed the SAV?

National Guard
Team:

FTL/PSA
Name:

Other (e.g., SME)
Name:



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



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

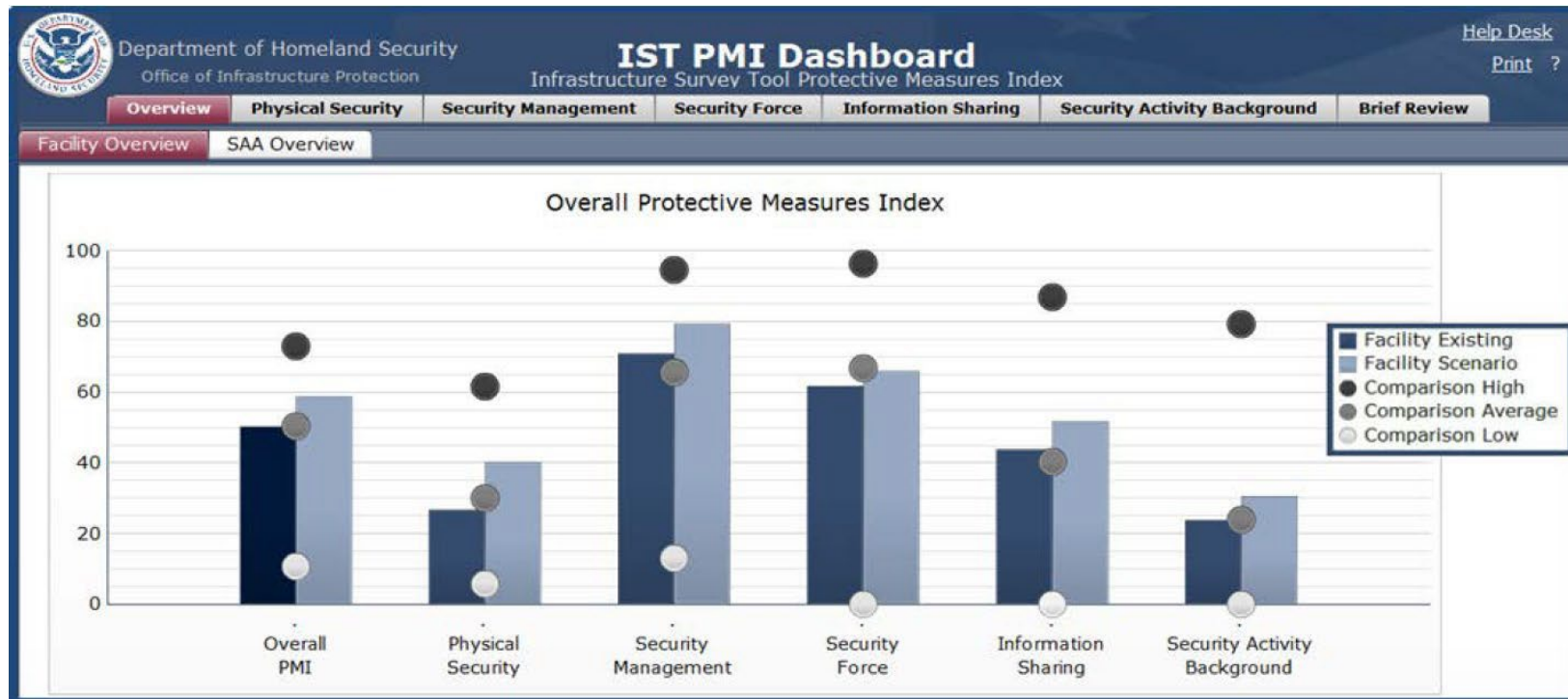
Dependencies (216)

- _____ 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.



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).

PMI Dashboard
Protective Measures Index

Print | Review | Help Desk

Overview | Physical Security | Security Management | Security Force | Information Sharing | Protective Measures

Physical Security

Select Various Measures to see their Effect on the CCTV Score

Does the facility utilize CCTV? No Yes

Coverage | Monitor | Record & Storage For... | **Camera Technolo...** | Anomaly Detecti...

Type

- Thermal
- Infrared
- Standard Analog
- Digital (IP)

Capability

- Color
- Black & White

Functionality: (Mark all that apply)

| Y | N |
|---|-----------------------|
| <input checked="" type="radio"/> Pan-til-Zoom | <input type="radio"/> |
| <input checked="" type="radio"/> Fixed | <input type="radio"/> |

Transmission Media: (Mark all that apply)

| Y | N |
|--|----------------------------------|
| <input type="radio"/> Wireless | <input checked="" type="radio"/> |
| <input checked="" type="radio"/> Coaxial | <input type="radio"/> |
| <input type="radio"/> Telephone wire | <input checked="" type="radio"/> |
| <input type="radio"/> Wire line (twisted pair) | <input checked="" type="radio"/> |
| <input checked="" type="radio"/> Fiber | <input type="radio"/> |

Emergency Backup Power

- Yes
- No

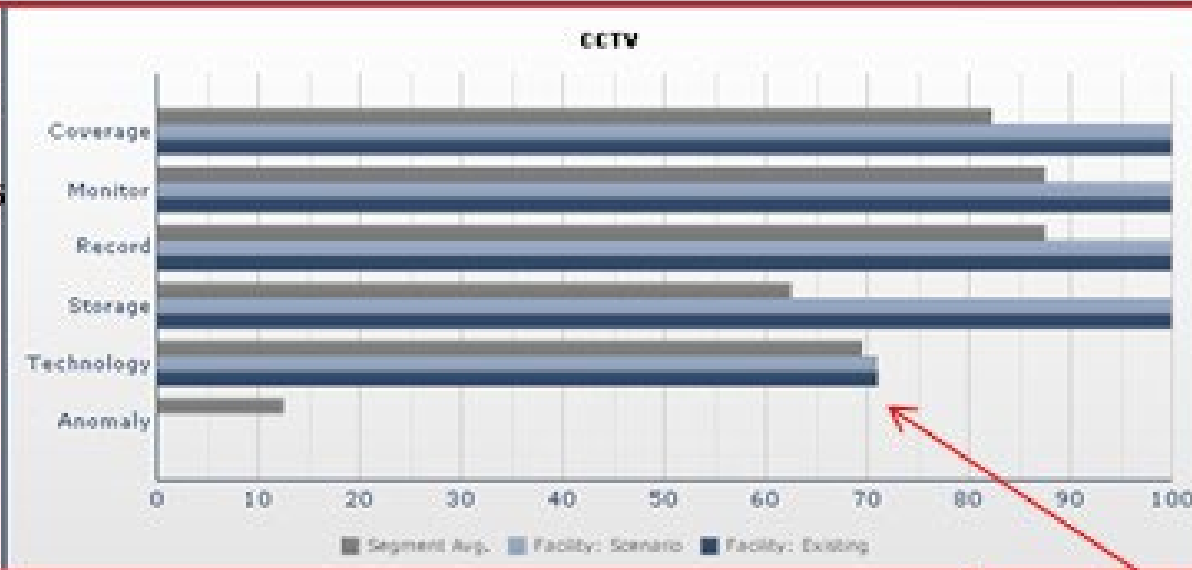
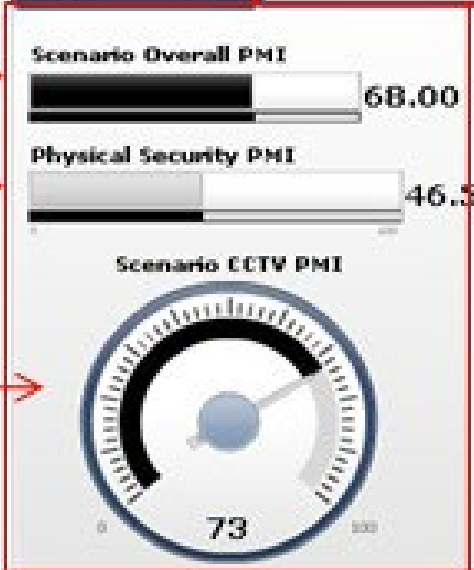
Level 3 Data

Level 2 Components

Overall PMI Bar

Level 1 PMI Bar

Level 2 PMI Dial



Tabs - Level 1

Level 3 Component PMI

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



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>

Pete Owen
December 1, 2023

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

Suspicious or Unattended?

Criminals or terrorists sometimes conceal improvised explosive devices (IEDs) in backpacks, suitcases, or common items.

Use this process to safely determine if an item is a serious threat or just unattended.

Is it **HOT**?

Hidden

- Placed out of sight
- Appears purposely concealed

Obviously suspicious

- Unexplainable wires or electronics
- Bomb-like components

not Typical

- Out of place for the location
- Priority related to a threat



Use R.A.I.N.

YES
(Suspicious)

NO
(Unattended)

- Treat with caution
- Try to determine the owner
- Report to an authority

If an item is suspicious you should:



R

Recognize the Indicators of a Suspected Explosive Device

Indicators can be related to the characteristics, events, location, or time, including whether the item is Hidden, Obviously suspicious, or not Typical (HOT).



A

Avoid the Area

Don't touch the suspected item. Instead, immediately move and direct others to move away immediately.



I

Isolate the Suspected Item

Establish a perimeter to secure the area and continue to direct people away. Use frontal and overhead cover and if available wear personal protective equipment.



N

Notify Appropriate Emergency Services

Describe the Suspicious items and persons, the person's Actions, the Location of the item, the Time of placement and discovery, and Your actions to mitigate risk (SALTY).

If you **see** something, **say** something®

REPORT SUSPICIOUS ITEMS

Contact local law enforcement or 9-1-1 in case of emergency



DEFEND TODAY. SECURE TOMORROW.

® If you see something, say something® used with permission of the U.S. Department of Homeland Security.

SUSPICIOUS MAIL OR PACKAGES

Protect yourself, your business, and your mailroom.

If you receive a suspicious letter or package:

- Stop. Don't handle.
- Isolate it immediately.
- Don't open, smell, or taste.
- Activate your emergency plan. Notify a supervisor.



If you suspect the mail or package contains a bomb (explosive), or radiological, biological, or chemical threat:

- Isolate area immediately
- Call 911
- Wash your hands with soap and water



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

Pete Owen
December 1, 2023

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



- Bomb Threat
- Bomb Searches

- Surviving a Bombing Attack
- Suspicious or Unattended Item



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

Pete Owen
December 1, 2023

Cyber Security Resources

- Cyber Security Advisors
- Vulnerability Scanning
- Cybersecurity Evaluation Tool

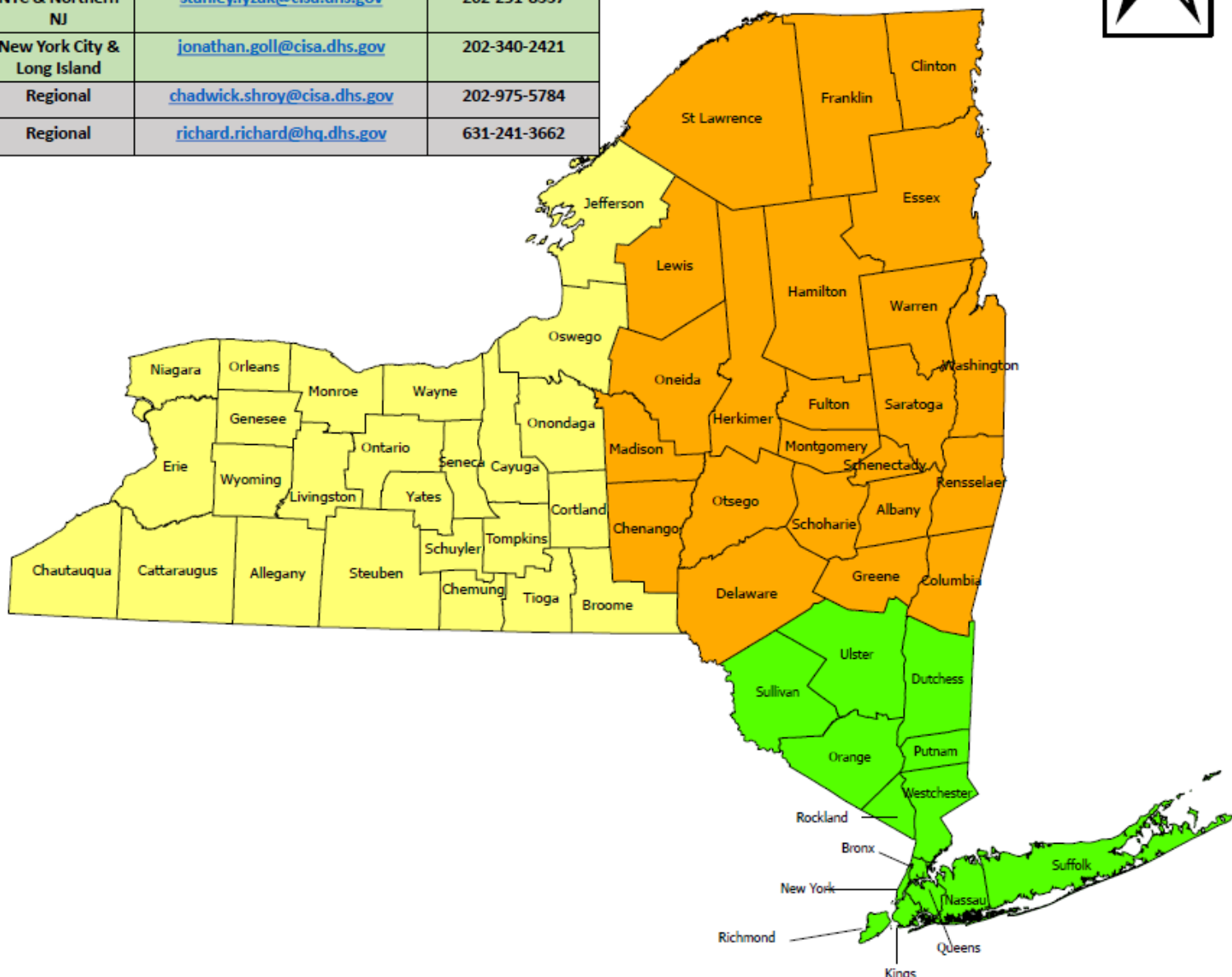


Cyber Security Advisors

- 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

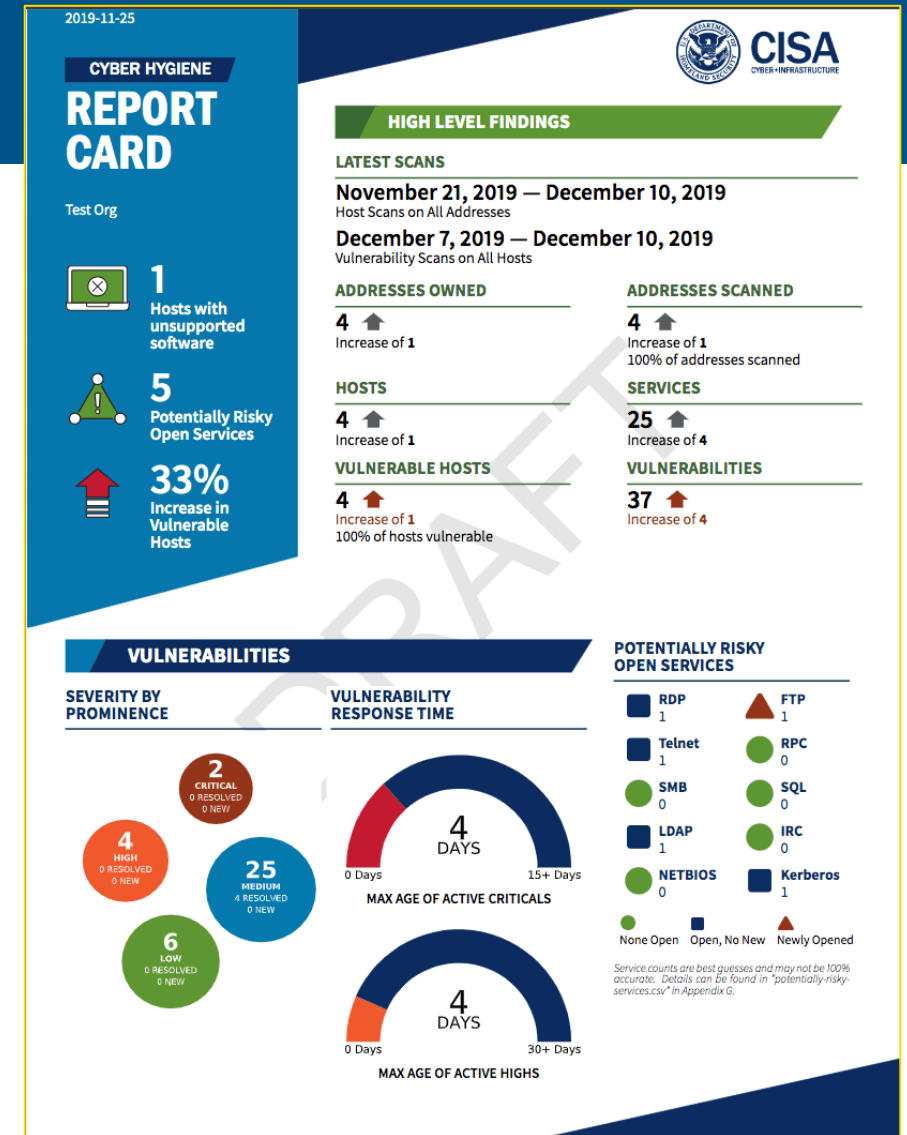
- Assesses control system and information system security against industry standards
- Self-Administered, undertaken independently
- Benefits:
 - Immediately available for download
 - Standards based
 - Ability to drill down on specific areas and issues

<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>

Pete Owen
December 1, 2023

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](https://www.cisa.gov)

Questions?

Email: peter.owen@hq.dhs.gov

Phone: (619) 733-9262