CYBERSECURITY LANDSCAPE AND OPERATIONAL RESILIENCE

Jason Burt
Cybersecurity Advisor, Region IV
Cybersecurity Advisor Program
Cybersecurity and Infrastructure Security Agency

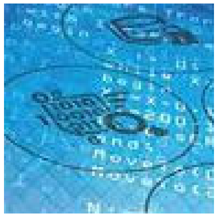
Divisions of CISA

- CISA consists of:

Cybersecurity Division

Infrastructure Security Division

Emergency Communications Division



National Risk Management Center

CISA Mission and Vision

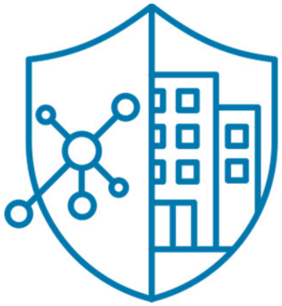
Cybersecurity and Infrastructure Security Agency (CISA)

Mission:

- Lead the collaborative national effort to strengthen the security and resilience of America’s critical infrastructure

Vision:

- A Nation with secure, resilient, and reliable critical infrastructure upon which the American way of life can thrive

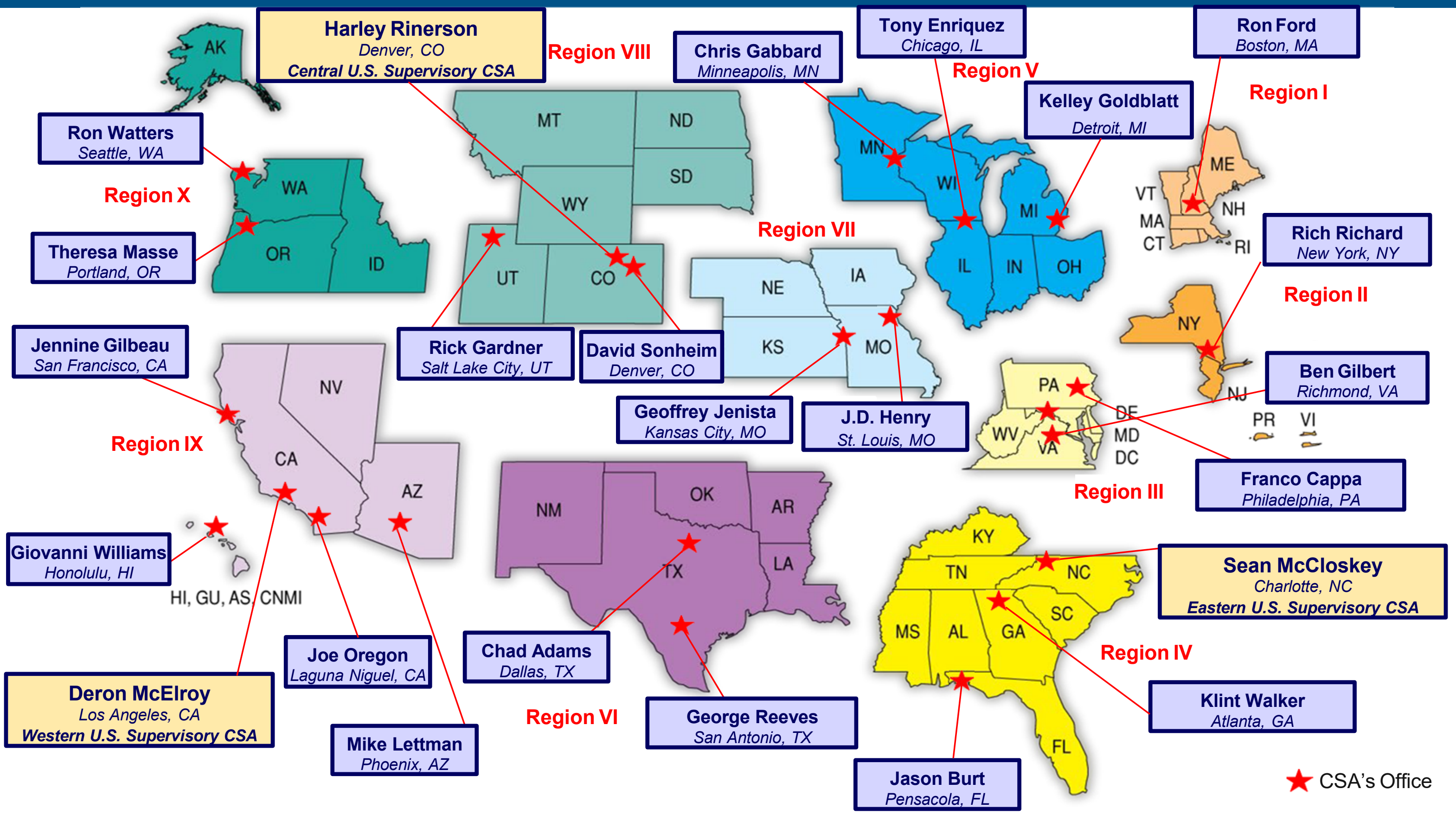


Jason Burt
December 10, 2020

CYBERSECURITY ADVISOR PROGRAM

Jason Burt
December 10, 2020

CSA Deployed Personnel



Harley Rinerson
Denver, CO
Central U.S. Supervisory CSA

Region VIII

Chris Gabbard
Minneapolis, MN

Tony Enriquez
Chicago, IL

Region V

Ron Ford
Boston, MA

Kelley Goldblatt
Detroit, MI

Region I

Ron Watters
Seattle, WA

Region X

Theresa Masse
Portland, OR

Region VII

Rich Richard
New York, NY

Region II

Jennine Gilbeau
San Francisco, CA

Rick Gardner
Salt Lake City, UT

David Sonheim
Denver, CO

Geoffrey Jenista
Kansas City, MO

J.D. Henry
St. Louis, MO

Ben Gilbert
Richmond, VA

Region IX

Region III

Franco Cappa
Philadelphia, PA

Giovanni Williams
Honolulu, HI

Sean McCloskey
Charlotte, NC
Eastern U.S. Supervisory CSA

Joe Oregon
Laguna Niguel, CA

Chad Adams
Dallas, TX

Region IV

Deron McElroy
Los Angeles, CA
Western U.S. Supervisory CSA

Klint Walker
Atlanta, GA

Region VI

George Reeves
San Antonio, TX

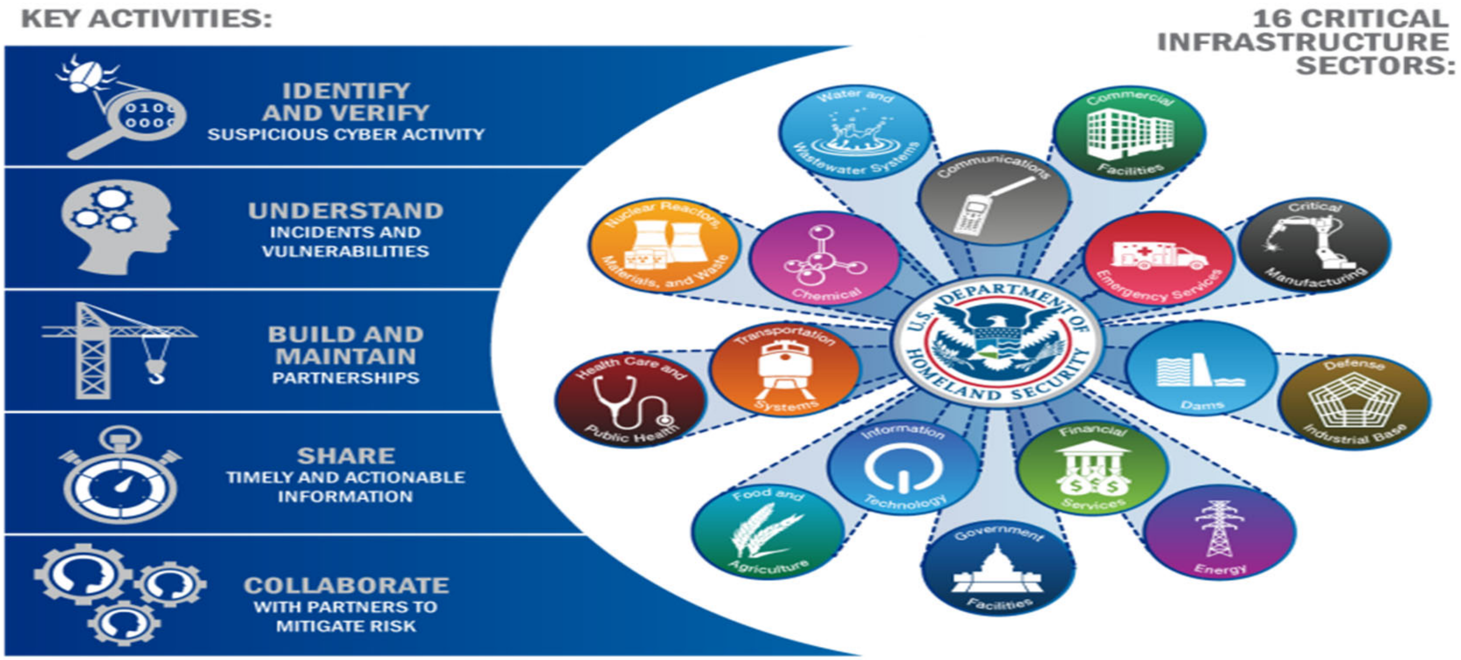
Mike Lettman
Phoenix, AZ

Jason Burt
Pensacola, FL

★ CSA's Office

Jason Burt
December 10, 2020

Serving Critical Infrastructure



Jason Burt
December 10, 2020

CYBER THREATS

Cyber Threats

COVID-19 Research

Adversaries could attempt to:

- **Delay or inhibit** the ability to **produce & deliver** viable countermeasures
- **Disrupt critical systems** for illicit financial gain
- **Undermine confidence** in the US COVID response efforts and trust the final vaccines or countermeasures

To achieve these goals, they may

- **Steal Intellectual Property**
  - Research, clinical trials, manufacturing & scale-up
- **Tamper** with, **destroy**, or **deny access** to data & systems (e.g. clinical data, SCADA systems)
- **Discredit** the veracity of scientific research and related organizations, persons

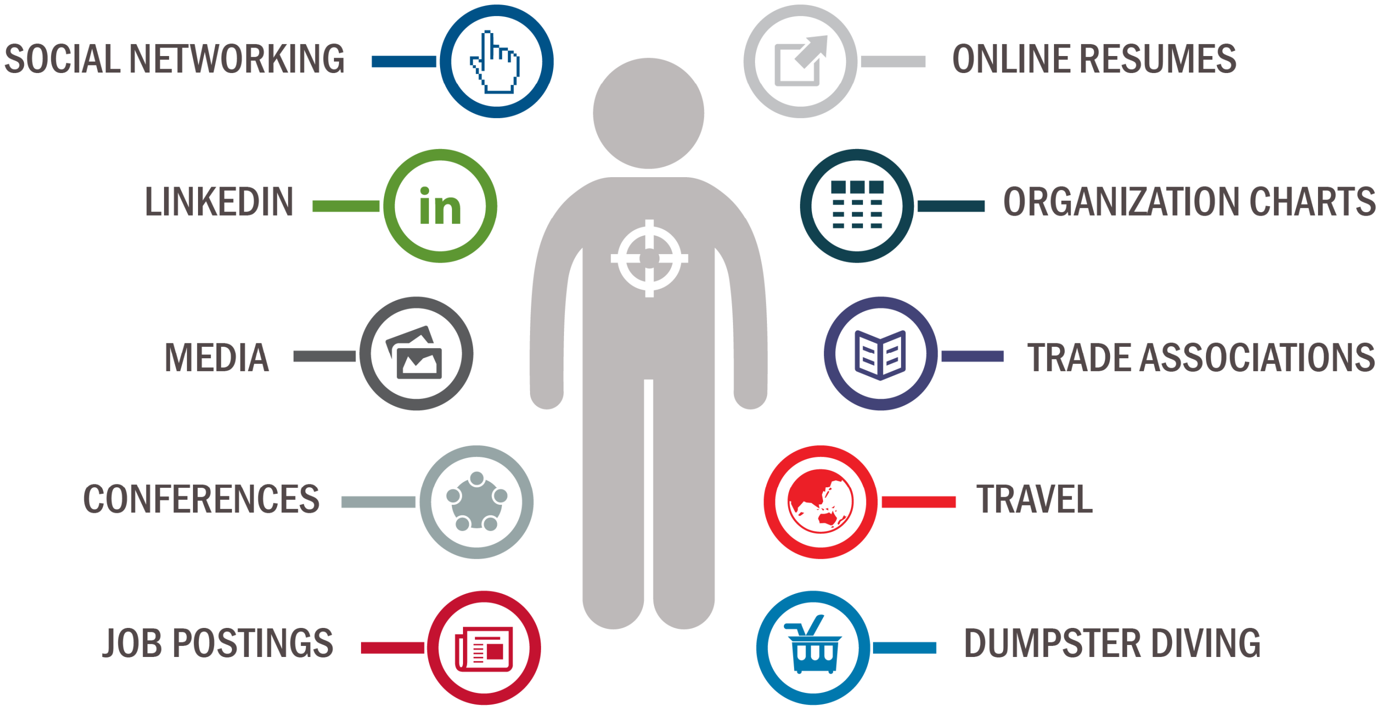
Targets

- **R&D for vaccines** (Vx), therapeutics (Tx,) and diagnostics (Dx)
- R&D for **technology, manufacturing, and scaling** of Vx, Tx, and Dx
- Vaccine **components** and **manufacturing techniques**
- **Cyber-Physical systems** for manufacturing, fill finish, & **Cold Storage**
- **Clinical trial data** and results
- Candidate **submission data** & communications
- Personal devices & accounts of **high-value individuals**

Threat Vectors

- ➢ Phishing
  - Masquerading as CDC, WHO official comms
- ➢ Spear-phishing
- ➢ Exploiting unpatched vulnerabilities on web-facing systems
  - Especially remote-access (e.g. VPN, RDP)
- ➢ Exploiting third-parties (e.g. managed services)
- ➢ Web shells
- ➢ Compromising home networks of employees or family members via emails & telework applications
- ➢ Focus on remote / collaboration platforms (O365, Webex, Google Drive credentials)
- ➢ Insider Threat

How Are You Targeted?



SOCIAL NETWORKING

LINKEDIN

MEDIA

CONFERENCES

JOB POSTINGS

ONLINE RESUMES

ORGANIZATION CHARTS

TRADE ASSOCIATIONS

TRAVEL

DUMPSTER DIVING

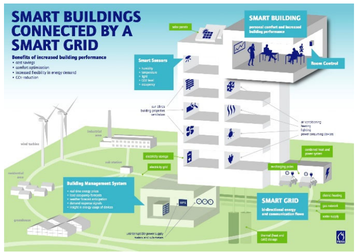
Cybersecurity is Critical

- Smart cars, electrical grids, medical devices, manufacturing, homes, buildings, smart everything!
- We bet our lives on these systems

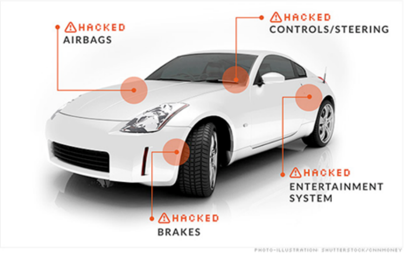
cyber security ⇔ physical safety!

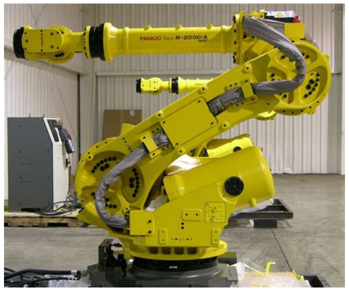
- Yet, much of CPS are “cobbled together from stuff found on the Web”!

Our buildings


SMART BUILDINGS CONNECTED BY A SMART GRID
Benefits of increased building performance
• cost savings
• comfort optimization
• increased flexibility in energy demand
• CO2 reduction
SMART BUILDING
personal comfort and increased building performance
solar panels
Smart Sensors
• humidity
• temperature
• light
• CO2 level
• occupancy
Room Control
sun blinds
building properties
ventilation
air conditioning
heating
lighting
power consuming devices
wind turbine
industrial area
sub station
residential area
greenhouse
electricity storage
electricity grid
combined heat and power system
ev-charging poles
Building Management System
• real time energy prices
• load occupancy forecasts
• weather forecast anticipation
• demand response signals
• insight in energy usage of devices
UPS
uninterruptible power supply
meters and sub-meters
SMART GRID
bi-directional energy and communication flows
district heating
gas network
water supply
thermal (heat and cold) storage
PRIVA

Our transport

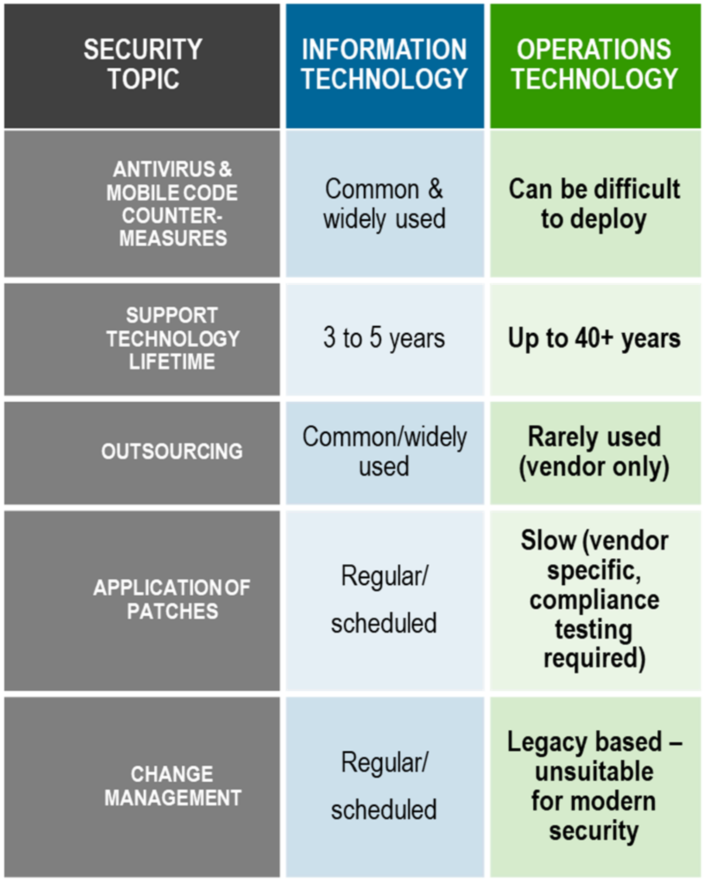




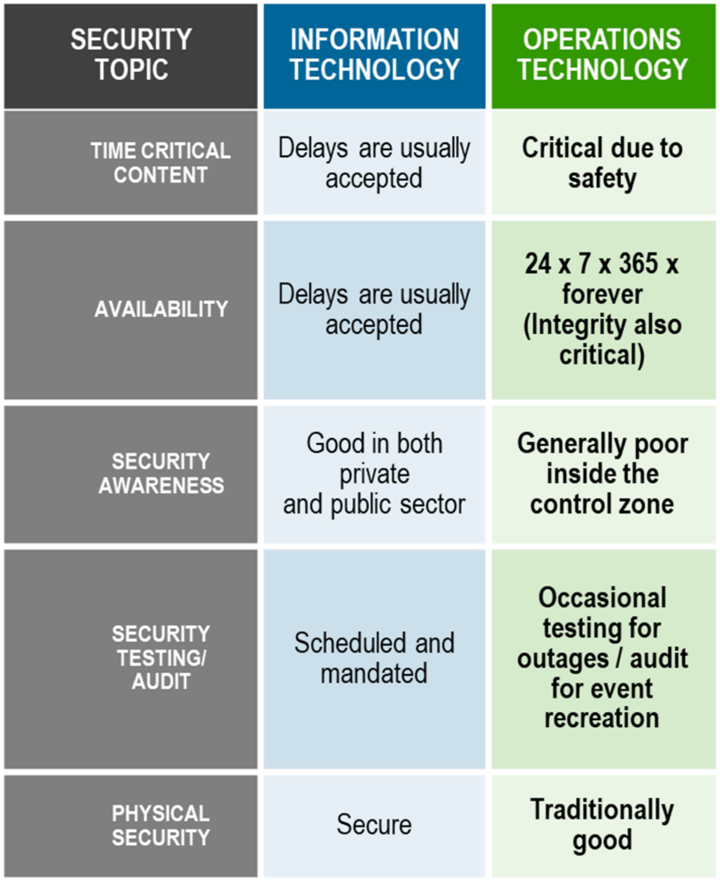
Our Production

Our health

IT vs OT



SECURITY TOPIC	INFORMATION TECHNOLOGY	OPERATIONS TECHNOLOGY
ANTIVIRUS & MOBILE CODE COUNTER-MEASURES	Common & widely used	**Can be difficult to deploy**
SUPPORT TECHNOLOGY LIFETIME	3 to 5 years	**Up to 40+ years**
OUTSOURCING	Common/widely used	**Rarely used (vendor only)**
APPLICATION OF PATCHES	Regular/ scheduled	**Slow (vendor specific, compliance testing required)**
CHANGE MANAGEMENT	Regular/ scheduled	**Legacy based – unsuitable for modern security**



SECURITY TOPIC	INFORMATION TECHNOLOGY	OPERATIONS TECHNOLOGY
TIME CRITICAL CONTENT	Delays are usually accepted	**Critical due to safety**
AVAILABILITY	Delays are usually accepted	**24 x 7 x 365 x forever (Integrity also critical)**
SECURITY AWARENESS	Good in both private and public sector	**Generally poor inside the control zone**
SECURITY TESTING/ AUDIT	Scheduled and mandated	**Occasional testing for outages / audit for event recreation**
PHYSICAL SECURITY	Secure	**Traditionally good**

Recent Events

- In 2017, NotPetya Ransomware cost a major Bio-Pharma company $310 MM
- March 2020 announcement by FBI/CISA on Chinese actors targeting COVID-19 research organizations
- TA505, the financially-motivated criminal group behind Locky ransomware and Dridex banking Trojan, has been targeting the U.S. healthcare, manufacturing, and pharma industry with ransomware.
- Fortinet reported a spear-phishing campaign against medical device suppliers featuring a subject line “Inquiry on Medical Supplies” with a malicious Word attachment.
- APT29 (Cozy Bear) targeting COVID-19 vaccine development
- FBI indicted two U.S.-based Chinese hackers who targeted COVID-19 vaccine developers

Sources:

- https://www.proofpoint.com/us/blog/threat-insight/ta505-and-others-launch-new-coronavirus-campaigns-now-largest-collection-attack
- https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development
- https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion

Recommendations

- ➢ Train & protect employees against phishing & email-based attacks
- ➢ Patch public-facing systems quickly
- ➢ Enforce MFA
  - Especially on remote access (VPN, etc.)
- ➢ (Off-box) Logging & monitoring access & usage logs of critical assets
- ➢ Reduce & monitor admins & admin privileges (granular access control)
- ➢ Enforce strong passwords & password rotation
- ➢ Ensure regular, robust, and offsite/offline backups of all critical decision data
- ➢ [Manufacturing] Logically or physically isolate OT from IT networks

CISA CYBER SERVICES

Range of Cybersecurity Services

STRATEGIC
(C-Suite Level)

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

TECHNICAL
(Network-Administrator Level)

Jason Burt
December 10, 2020

Protected Critical Infrastructure Information Program

Protected Critical Infrastructure Information (PCII) Program Guards Your Information

- Sensitive critical infrastructure information voluntarily given to CISA is protected by law from
  - Public release under Freedom of Information Act requests,
  - Public release under State, local, tribal, or territorial disclosure laws,
  - Use in civil litigation and
  - Use in regulatory purposes.

Jason Burt
December 10, 2020

Contact

Additional Information

CyberAdvisor@cisa.dhs.gov

CISA Contact Information

Jason Burt Region IV Cybersecurity Advisor (Alabama, Mississippi, Florida)	Jason.Burt@cisa.dhs.gov (202) 578-9954 (Cell)
Klint Walker Region IV Cybersecurity Advisor (Georgia, Tennessee, Kentucky)	Klint.Walker@hq.dhs.gov (404) 895-1127 (Cell)
Sean McCloskey Region IV Cybersecurity Advisor (North Carolina, South Carolina)	Sean.McCloskey@hq.dhs.gov (202) 578-8853 (Cell)