CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

CISA Update

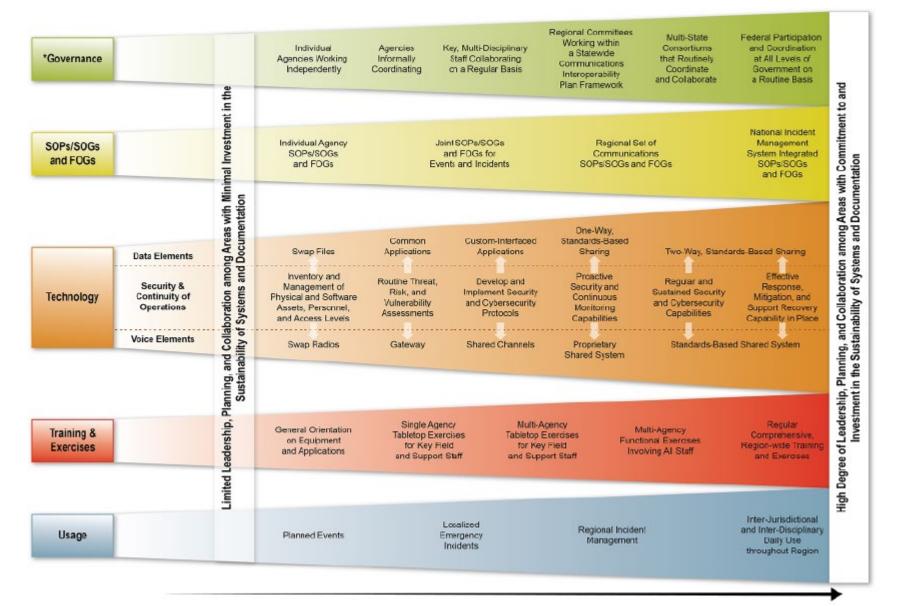
James Lundsted, Emergency Communications Coordinator Emergency Communications Division



Louisiana Statewide Interoperability Executive Committee (SIEC) Interoperable Communications



Updated SAFECOM Interoperability Continuum





SOPs/SOGs and FOGs		Areas with Minimal Investment in the ocumentation	Individual Agency SOPs/SOGs and FOGs	Joint SCPs/SOGs and FDGs for Events and Incidents		Regional Set of Communications SOPs/SOGs and FOGs		National Incident Management System Integrated SOPsISOGs and FOGs
	Data Elements	nning, and Collaboration among Areas with Mi Sustainability of Systems and Documentation	Swap Files	Common Applications	Custom-Interfaced Applications	One-Way, Standards-Based Sharing	Two-Way, Standar	rds-Based Sharing
Technology	Security & Continuity of Operations	boration among Systems and Do	inventory and Management of Physical and Software Assets, Personnel, and Access Levels	Routine Threat, Risk, and Vulnerability Assessments	Develop and Implement Security and Cybersecurity Protocols	Proactive Security and Continuous Monitoring Capabilities	Regular and Sustained Security and Cybersecurity Capabilities	Effective Response, Mitigation, and Support Recovery Capability in Place
	Voice Elements	ing, and Colk	Swap Radios	Gateway	Shared Channels	Proprietary Shared System	Standards-Base	d Shared System
Training & Exercises		Limited Leadership, Planning, and Collaboration Sustainability of Systems	General Orientation on Equipment and Applications	Single Agency Multi-As Tabletop Exercises Tabletop E for Key Field for Key and Support Staff and Supp		terdises Fund	lulti-Agency tional Exercises owing Al Staff	Regular Comprehensive, Region-wide Training and Exercises
Usage		Planned Events	Localized Emergency Incidents		Regional Incident Management		Inter-Jurisdictional and Inter-Disciplinary Daily Use throughout Region	

A Closer Look at the Technology Lane

Technology

Technology	Data Elements	Swap Files	Common Applications	Custom-Interfaced Applications	One-Way, Standards-Based Sharing	Two-Way, Standards-Based Sharing	
	Security & Continuity of Operations	Inventory and Management of Physical and Software Assets, Personnel, and Access Levels	Routine Threat, Risk, and Vulnerability Assessments	Develop and Implement Security and Cybersecurity Protocols	Continuous	Regular and Sustained Security and Cybersecurity Capabilities	Effective Response, Mitigation, and Support Recovery Capability in Place
	Voice Elements	Swap Radios	Gateway	Shared Channels	Proprietary Shared System	Standards-Based Shared System	



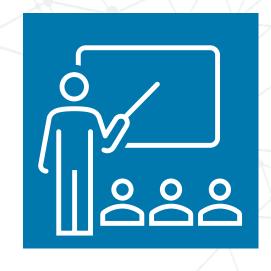


Threat of Cyber Attacks

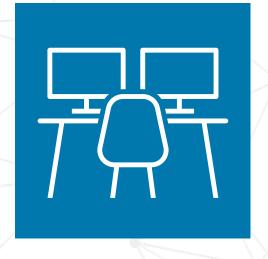
Cybersecurity Services



Response Assistance



Cybersecurity Advisors



Preparedness Activities



CSET Tool Ransomware Readiness Assessment



About



CYBER SECURITY EVALUATION TOOL

Version: 10.2.0.0

https://github.com/cisagov/cset

cset@dhs.gov



Cybersecurity & Infrastructure Security Agency

Contact

To learn more about cyber vulnerabilities, training, standards, and references, visit the Vulnerability Management US-CERT website or contact vulnerability@cisa.gov.

CISA, Cybersecurity and Infrastructure Security Agency, encourages you to report suspicious cyber activity, incidents,

CSET Training Resources

CSET training is available through the following resources:

User Guide

Video Tutorials

https://www.youtube.com/c/CSETCyberS ecurityEvaluationTool

CISA Cybersecurity Training Program

The training program events consist of Web-Based Training courses, 'regional' training courses and workshops at venues in various locations, in addition to the 5-day training event held in Idaho Falls, Idaho.

Note: All training courses are presented at no cost to the attendee.

Training Website:

https://us-cert.cisa.gov/ics/Training-Available-Through-ICS-CERT



CSET Capabilities



What CSET CAN do:

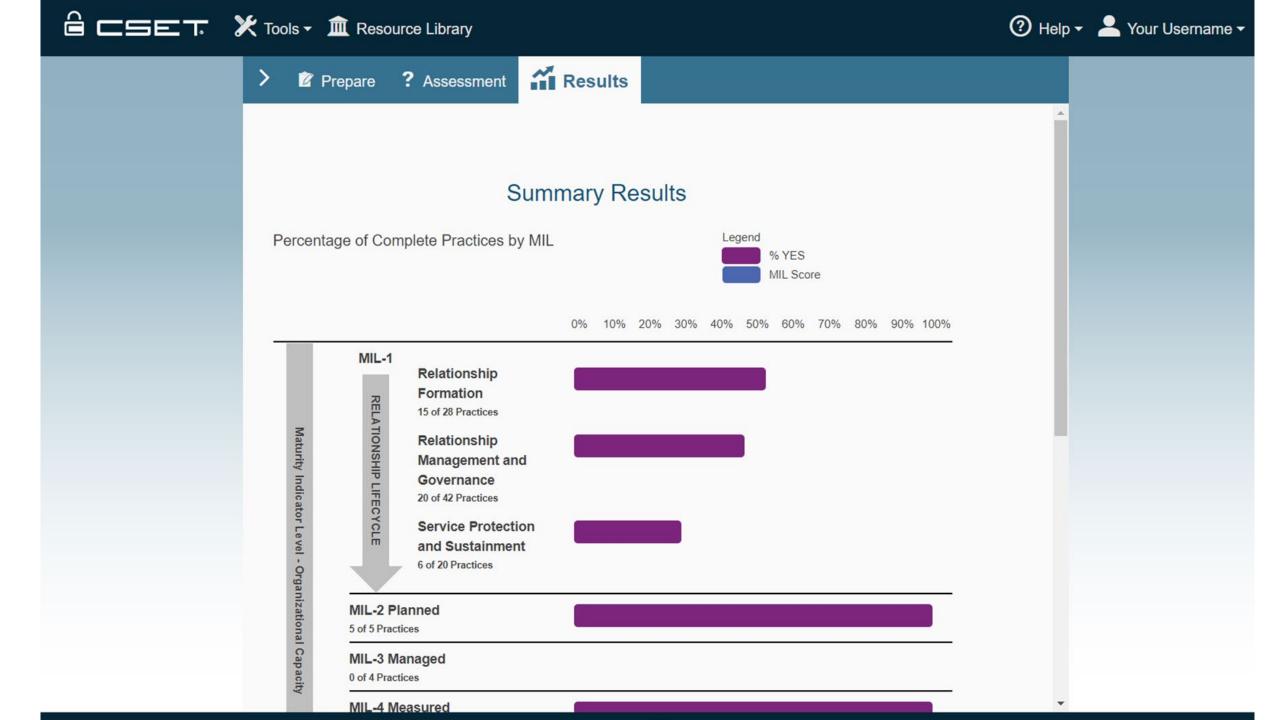
- Provide a consistent means of evaluating a control system network as part of a comprehensive cybersecurity assessment
- Specify cyber security recommendations
- Report using standards-based information analysis
- Provide a baseline cybersecurity posture



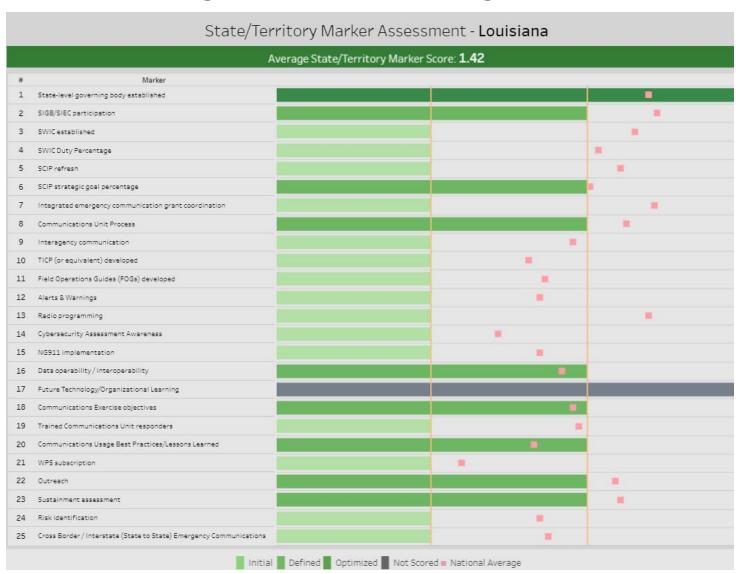
What CSET CAN'T do:

- Validate accuracy of user inputs
- Ensure compliance with organizational or regulatory cybersecurity policies & procedures
- Ensure implementation of cybersecurity enhancements or mitigation techniques
- Identify all known cybersecurity vulnerabilities





Interoperability Capability Measurements





State/Territory Marker Assessment - Louisiana





FY21 Technical Assistance



Support for in-person courses, exercises is transitioning Likely the Incident Tactical Dispatcher, Incident Communications Center Manager will continue as virtual deliveries. AUXCOMM may continue as both virtual or in-person.



Operational efficiencies being explored: discontinue printing of student guides?

cisa.gov/publication/ictapscip-resources

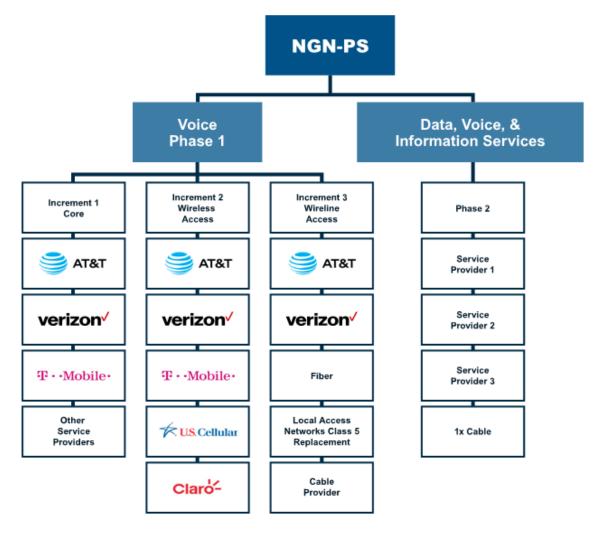


What's Next: Evolving Priority Services





Next Gen Priority Services Program











Questions?

Jim Lundsted

Emergency Communications Coordinator -

Regions 6 & 7

Email: <u>James.Lundsted@cisa.dhs.gov</u>

Phone: 202-630-1177

