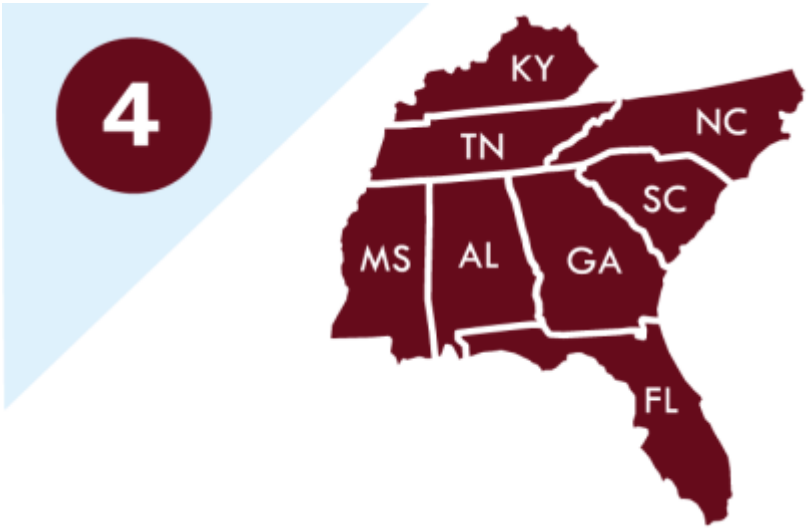
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Region 4 Stakeholder Update

January 2025



Welcome to the Stakeholder Update

Julius Gamble, Regional Director

I am excited to share with you Region 4's first Stakeholder Update. As we publish this first edition, I'd like to tell you what led to its creation.

We know that news flies fast for the more than 66 million people across the 6 Tribal Nations and 8 states that makeup Region 4. Through our Stakeholder Update we intend to provide you with timely, actionable information from across CISA and Region 4 in one place.

You will find information about upcoming trainings, events, and notifications about CISA publications in the following sections. We have also included a section to assist you in keeping or getting in touch with one of your local advisors to learn more about our services.

Our aim is to make this a useful tool for you, our partners, and we welcome feedback and content suggestions. You can provide these to us by clicking the "Feedback Form" button below.

One more thing before you dig into our first update. Please click on the map of the region above to be taken to the subscription page, you will need to sign up there to continue to

receive our update. Enter your email address on the landing page and check the box for the “Region 4 Stakeholder Update” at the bottom of the subscriber preference page under the General tab.

Feedback Form

CISA In Your Neighborhood

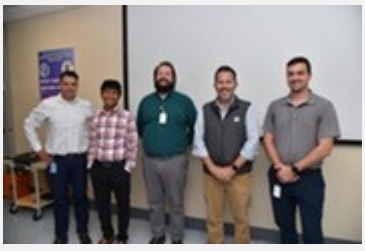
Tabletop Exercise Highlights the Importance of Low-Tech Options

On November 19, 2024, Regional Sector Outreach Coordinator Corinne Epstein facilitated a convergence tabletop exercise for the Tennessee Titians at their practice facility, Accension St. Thomas Sports Park in Nashville, TN.

The organization made quick work of the original scenario so the CISA team, including Cybersecurity Advisor Ryan Lewis, Protective Security Advisor Greg Innis, and Chemical Security Inspector Andrew Balter, pivoted to create challenging discussion questions on the spot. Through the discussion of the organizations’ extensive safety and security protocols, it became apparent that the reliance on technology was primary to the way they operated. Cybersecurity Advisor Lewis add some humor to the event by role playing a fan who didn’t use common devices, challenging the group to think outside the box.

At the conclusion of the exercise, the participants noted that creating a “war room” where everyone could discuss the situation and keeping hard copies of some critical documents on hand were two practices they would implement right away.

Cybersecurity Awareness Month Events Increase Partnership with County Government



The Information Technology Department in Guilford County, NC hosted two iterations of a Secure Our World: Guilford County's 2024 Cybersecurity Awareness Month event this past October.

The virtual session included a presentation by South Carolina Cybersecurity State Coordinator Anthony Carbone. While the in-person session included a presentation by North Carolina Cybersecurity State Coordinator Rob Main, who received a rave review from the county’s IT Security Manager.

Guildford County is home to Greensboro, which is the third most populous city in the state.

Training Opportunities

CISA Learning is now available!

CISA Learning has replaced the Federal Virtual Training Environment (FedVTE). It will continue to offer the same no cost online cybersecurity training as FedVTE on topics such as cloud security, ethical hacking and surveillance, risk management, malware analysis, and more.

Partners can access the new system using this link: **CISA Learning**

Please reference the CISA Learning page for the latest information.

Advancing Campus Safety & Resilience Webinar

The U.S. Department of Homeland Security (DHS) invites U.S Colleges and Universities, Historically Black Colleges and Universities (HBCUs), and other Minority Serving Institutions (MSIs) to join a webinar on **February 6, 2025 from 11:30 am to 1 pm EST.**

This event will provide updates on DHS programs, initiatives, and available resources to improve campus resilience. DHS staff will share information about security planning, provide an overview of resilience hubs for campuses and surrounding communities, and discuss grants and resources available to local communities to ensure the safety and security of their institutions. This webinar is intended for college and university administrators, public safety and campus law enforcement officials, student affairs/student life representatives, interested faculty, emergency managers, and other individuals and offices that have a role in supporting community safety and the wellbeing of students.

Registration Form

Drone Assessment and Response Tactics (DART)

February 6, 2025 8 am to 4 pm ET- In Person: Augusta, GA

The DART course provides emergency personnel with the knowledge and skills necessary to detect, identity, track, assess, respond, and report Unmanned Aircraft Systems (UAS) activity.

Participants are presented with information on the current UAS criminal and terrorist threat, analog and electronic UAS detection techniques, and response tactics to address this threat.

Recommended Audience: Emergency Management, Emergency Medical Services, Fire Service, and Law Enforcement.

Registration Form

Industrial Control Systems (ICS) Training

CISA offers free, virtual ICS trainings geared toward Critical Infrastructure owners and operators. The trainings are designed to reduce cybersecurity risks to critical infrastructure and encourage cooperation between CISA and the private sector.

Trainings vary in length and run from 8:00 a.m. – 5:00 p.m. MST (10:00 a.m. – 7:00 p.m. EST). The schedule can be accessed on the **ICS Training Calendar** page.

Additional three- or four-day, in-person courses are offered at Idaho National Labs (INL) in Idaho Falls, ID. We are currently working to bring these courses to the region. Please contact us if you are interested in the in-person courses.

CISA Incident Response Training

January 15, 16 or 17, 2025 9 am to 1 PM ET

Instrumenting the Environment to Detect Suspicious and Malicious Activity Cyber Range Training (IR214) **Register Here**

January 16, 2025 9 am to 1 PM ET

Preventing DNS Infrastructure Tampering Cyber Range Training (IR206) **Register Here**

January 22, 2025 11 am to 12 PM ET

Understanding Indicators of Compromise (IR108) **Register Here**

February 6, 2025 12 p.m. to 4 p.m. EST

Preventing Web & Email Server Attacks Cyber Range Training **Register Here**

February 11, 2025 9 a.m. to 1 p.m. ET

Understanding Indicators of Compromise Cyber Range Training **Register Here**

Courses are published continuously on the **CISA Incident Response Training Page**

Office For Bombing Prevention Virtual Instructor Led Training

The Office for Bombing Prevention (OBP) and the Center for Domestic Preparedness have partnered to provide bombing prevention awareness learning opportunities for first responders, public safety personnel, and private sector partners through Virtual Instructor-Led Training (VILT). VILT courses provide basic bombing prevention information ranging from IED construction and classification to the terrorist attack cycle.

OBP VILT courses are continually offered, please see the **Course Schedule** for details.

National Notification Highlights

CISA Releases 2024 Year in Review

We are pleased to share the 2024 CISA Year in Review, which invites readers to learn about CISA's work over the past year and dive deeper into each topic through related links and videos. We are grateful to all our partners across industry, government at all levels, international partners, and beyond, whose strong collaboration contributed to a wide array of achievements across CISA's broad cybersecurity, infrastructure security, and emergency communications missions.

December 3, 2024

CISA and Partners Publish Guide to Protect Communications Infrastructure Against PRC Actor

December 10, 2024

CISA Releases De-escalation Action Guide

December 13, 2024

Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems

December 17, 2024

Playbook for Strengthening Cybersecurity in Federal Grant Programs for Critical Infrastructure

December 18, 2024

Mobile Communications Best Practices Guidance

January 7, 2025

CISA Releases IT and Product Design Sector-Specific Goals

January 10, 2025

CISA Releases Cybersecurity Performance Goals (CPG) Adoption Report

January 13, 2025

CISA Releases Secure by Demand: Priority Considerations for Operational Technology Owners and Operators When Selecting Digital Products

January 14, 2025

CISA and JCDC Release AI Cybersecurity Collaboration Playbook

Full Listing of CISA Advisories & Alerts

Regional Advisors

CISA has experts around the country to support critical infrastructure owners and operators and state, local, tribal, and territorial partners where they are. In order to build

stakeholder resiliency and form partnerships, these field personnel assess, advise, and assist and provide a variety of risk management and response services.

Protective Security Advisors (PSA)

Trained subject matter experts in critical infrastructure protection and vulnerability mitigation. They facilitate local field activities in coordination with other DHS offices and federal agencies. They also advise and assist state, local, tribal, and territorial (SLTT) officials and critical infrastructure owners and operators, and provide coordination and support in times of threat, disruption, or attack.

Cybersecurity Advisors (CSA)

Offer cybersecurity assistance to critical infrastructure owners and operators and SLTT officials. They introduce organizations to various CISA cybersecurity products and services, along with other public and private resources, and act as liaisons to CISA cyber programs. They can provide cyber preparedness assessments and protective resources, working group support, leadership, partnership in public-private development, and coordination and support in times of cyber threat, disruption, or attack.

Chemical Security

Manage programs to help stakeholders—private industry, public sector, and law enforcement—secure chemical facilities from many threats, ranging from: cyberattacks, insider threats, and theft and diversion for use in chemical or explosive weapons.

Contact Your Local Advisor