Critical Infrastructure Outreach

October 23, 2024

Fiscal Year 2024 Report to Congress

Homeland Security

Cybersecurity and Infrastructure Security Agency

Message from the Director of the Cybersecurity and Infrastructure Security Agency

October 23, 2024

The Cybersecurity and Infrastructure Security Agency (CISA) prepared the following report, "Critical Infrastructure Outreach," pursuant to a requirement in the Fiscal Year (FY) 2024 Department of Homeland Security (DHS) Appropriations Act (P.L. 118-47).

CISA is the operational lead for federal cybersecurity and the National Coordinator for critical infrastructure security and resilience. The agency works with partners to defend against today's threats and collaborates to build more secure and resilient infrastructure for the future. Partnership and collaboration with sector partners are essential to effectively executing CISA's mission to understand, manage, and reduce risks to the nation's cyber and physical infrastructure.

This report is provided to the following Members of Congress:

The Honorable Mark Amodei
Chairman, House Appropriations Subcommittee on Homeland Security

The Honorable Lauren Underwood
Ranking Member, House Appropriations Subcommittee on Homeland Security

The Honorable Chris Murphy
Chair, Senate Appropriations Subcommittee on Homeland Security

The Honorable Katie Britt
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

If you have any questions, please contact CISA Legislative Affairs at CISA_OLA@cisa.dhs.gov.

Sincerely,

Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency

Executive Summary

Partnership and collaboration with sector partners are essential to effectively executing CISA's mission to understand, manage, and reduce risks to the nation's cyber and physical infrastructure. CISA pursues a whole-of-nation approach for critical infrastructure security and resilience including sector outreach and engagement and coordination with partners.

As required by Congress, CISA has prepared this report to provide Congress with a detailed accounting of all the agency's mechanisms, programs, and initiatives that facilitate outreach to critical infrastructure owners and operators.

Sector partnership and engagement is central to CISA executing its mission. Operational collaboration is highlighted as one of the four major goals in CISA's 2023-2025 Strategic Plan. Congress asked CISA to specifically outline its sector outreach mechanisms, programs, and initiatives at the national, regional, and local levels. It is important to note that CISA develops its programs and initiatives to be used by all stakeholders across the nation. For this report, programs and initiatives with a specific regional, state, local, tribal, and territorial (SLTT), or community focus are identified in separate sections.

One of CISA's primary mechanisms to conduct public-private outreach is through convening national-level coordinating councils and collaborative groups that bring together partners from federal and SLTT governments, regional entities, the private sector, and non-governmental organizations to collaborate on critical infrastructure security and resilience programs and approaches, and to achieve national goals and objectives. These councils provide primary organizational structures for coordinating critical infrastructure security and resilience efforts and activities within and across the 16 sectors.

CISA develops and leads outreach programs and initiatives for critical infrastructure owners and operators nationwide. These programs, tools, and trainings are intended to benefit CISA's partners and stakeholders across the nation by reducing risk to and enhancing critical infrastructure resilience. CISA often relies on regional staff and other key stakeholders to provide the resources and information to critical infrastructure owners and operators, including SLTT and interagency partners for a whole of government approach to risk management. CISA's programs and initiatives are focused on providing the information, capabilities, and support partners need to better respond to the changing risk environment. Because cybersecurity is a whole of government mission, CISA serves a unique role in collaborating closely with interagency partners.

Regionally, CISA delivers services to regional stakeholders through its 10 regional offices. These offices provide a range of cyber and physical services to support the security and resilience of critical infrastructure owners and operators, as well as SLTT partners, throughout the nation. CISA's regional staff increase access to CISA's products and services, build partnerships, and develop nationwide risk reduction and resiliency capacity. There are some programs specifically for execution at the regional level, and these are highlighted in the section.

While CISA's programs and initiatives are intended for all sector partners and stakeholders, some focus primarily on SLTT partners and stakeholders.

CISA is in the process of executing National Security Memorandum (NSM-22) requirements including those supporting sector cooperation, ensuring engagements are coordinated across partners, and enabling effective information sharing and outreach. One of the NSM-22 requirements is developing the 2025 National Infrastructure Risk Management Plan (National Plan) that will articulate how the federal government will collaborate with partners to identify and manage risk. The National Plan will replace the 2013 National Infrastructure Protection Plan, and its development and execution will rely on collaboration and cooperation with federal, SLTT, and private sector partners.

CISA continues to assess the needs of critical infrastructure owners and operators and regularly evaluates its programs, mechanisms, and initiatives related to critical infrastructure outreach.

Critical Infrastructure Outreach

Table of Contents

I. Legislative Language

The House Report 118-123, which accompanies the Fiscal Year (FY) 2024 Department of Homeland Security (DHS) Appropriations Act (P.L. 118-47), includes the following requirement.

> *Critical Infrastructure Outreach*. — Within 90 days of the date of enactment of this Act, the Committee directs CISA to submit a report detailing all mechanisms, programs, and initiatives CISA has in place to facilitate outreach to critical infrastructure owners and operators within the 16 critical infrastructure sectors including Sector Coordinating Councils. The report shall include an accounting of regular outreach activities carried out at the national level, in the different CISA regions, and any special initiatives related to rural, suburban, and urban areas. CISA must also provide information on the level of cooperation of critical infrastructure owners and operators and any recommendations, including legislative recommendations, to improve cooperation or adoption of security guidance and best practices to enhance homeland security. The report should also include any gaps or areas of overlap within these mechanisms, programs, and initiatives.

II. Background

The nation's critical infrastructure underpins all aspects of modern life and is essential for national security, economic vitality, and public health and safety. Critical infrastructure is owned and operated by public and private entities, meaning public-private partnership is essential for security and resilience.

The Cybersecurity and Infrastructure Security Agency (CISA) recognizes, however, that its security partnerships must result in action that drives positive change across cyberspace. As emphasized in the National Cybersecurity Strategy, the most capable and best-positioned partners must do more to make our digital ecosystem secure and resilient. CISA will ask more of these partners, so that we as a nation can minimize the burden on individual end users, small businesses, state and local governments, and critical infrastructure operators with limited resources. As the National Cybersecurity Strategy notes, "Our collective cyber resilience cannot rely on the constant vigilance of our smallest organizations and individual citizens…. Together, industry and government must drive effective and equitable collaboration to correct market failures, minimize the harms from cyber incidents to society's most vulnerable, and defend our shared digital ecosystem."[1]

CISA is the nation's cyber defense agency and National Coordinator for critical infrastructure security and resilience and is designed for collaboration and partnership. As described in House report 118-123 accompanying the FY 2024 Department of Homeland Security Appropriations Act (P.L. 118-47), CISA is "responsible for enhancing the security of the nation's cyber and physical infrastructure and interoperable communications systems; safeguarding and securing cyberspace; and strengthening national preparedness and resilience."

Effective outreach to critical infrastructure owners and operators is central to CISA fulfilling its mission and executing its distinct roles:

1. **National Coordinator**: CISA is responsible for leading the national effort to secure and protect critical infrastructure by coordinating with Sector Risk Management Agencies, relevant departments and agencies, the private sector, and state, local, tribal, and territorial (SLTT) partners.

2. **Sector Risk Management Agency (SRMA)**: CISA is the federal agency responsible for providing institutional knowledge and specialized expertise for eight critical infrastructure sectors and one subsector.

3. **Support Services Provider:** CISA has technical expertise in multiple areas of importance to critical infrastructure, which SRMAs may not have the capability or capacity to provide (e.g. physical security, cybersecurity, risk management, emergency communications, etc.). CISA can leverage its role as the National Coordinator for the Security and Resilience of Critical Infrastructure to coordinate with SRMAs and, as appropriate, other relevant departments and agencies to catalogue and provide

[1] Office of the National Cyber Director, the White House, National Cybersecurity Strategy (2023), p. 4, 5

capabilities, resources, and support services to enhance security and resilience efforts of SRMAs and critical infrastructure sector partners.

The agency's six divisions all have a role to play in executing its mission, particularly in facilitating critical infrastructure sector outreach:

- **Stakeholder Engagement Division (SED)**: SED leads CISA's national and international voluntary partnerships and engagements while serving as the agency's hub for the shared stakeholder information that unifies CISA's approach to whole-of-nation operational collaboration and information sharing. SED executes CISA's National Coordinator role, translating national priorities into actionable guidance and support to all 16 critical infrastructure sectors, as well as fulfilling CISA's statutory SRMA requirements for its assigned sectors.

- **National Risk Management Center (NRMC):** NRMC provides critical analytical support to CISA's mission to understand, manage, and reduce risk to the cyber and physical infrastructure Americans rely on daily. In support of CISA's SRMA role, NRMC is conducting risk analyses across eight sectors and one subsector. In support of CISA's National Coordinator role, NRMC provides cross-sector and emerging risk analysis in support of all critical infrastructure sectors. In support of CISA's shared services provider role, NRMC provides training, approaches, and tools for other national risk managers to conduct their analysis.

- **Integrated Operations Division (IOD):** IOD is responsible for maintaining situational awareness and delivering CISA services nationally. As the National Coordinator for the Security and Resilience of Critical Infrastructure, CISA is responsible for maintaining a common operating picture across the nation to ensure the protection and resilience of critical infrastructure. CISA's 24x7 watch, led by IOD, is integral in our awareness of vulnerabilities, threats, and on-going incidents where we receive and share information with our stakeholders and partners across the entire critical infrastructure community. Through the CISA Regions, IOD delivers support to stakeholders and partners across SLTT governments and the critical infrastructure community through:
    - Cyber and physical vulnerability assessments.
    - Architecture review and design subject matter expertise.
    - Incident response support.
    - Exercise planning and support.
    - National Special Security Event planning and support.
    - Emergency communication planning, strategy, training, and response.

- **Infrastructure Security Division (ISD):** Working closely with critical infrastructure owners/operators and SLTT partners, ISD leads the national effort to enhance the security and resilience of the nation's critical infrastructure and public gathering locations. ISD programs support stakeholder security capacity to help mitigate prevalent threats such as active shooter incidents, vehicle ramming, and risks posed by unmanned aircraft systems; lead DHS efforts to implement National Counter-Improvised Explosive Device (C-IED) policy and enhance the nation's ability to prevent the use of explosives against critical

infrastructure; provide guidance and identify resources to enhance the safety of schools and academic institutions; ensure dangerous chemicals located at the nation's high-risk chemical facilities are properly secured; and conduct cyber and physical exercises to enhance the security and resilience of critical infrastructure.

- **Cybersecurity Division (CSD):** CSD leads the national effort to reduce the prevalence and impact of cyber incidents by providing guidance, and capabilities that address immediate risks and advance the nation toward a secure cyber ecosystem. In support of this mission, CSD identifies, detects, assesses, and responds to urgent cybersecurity risks through information sharing, deployment of detective and preventive technologies, and by providing incident response and "hunt" capabilities to help the nation respond to and minimize the impacts of significant incidents. CSD also provides tools, services, and expert guidance to drive cybersecurity risk management and build resilience by addressing systemic risk and helping organizations operate safely and reliably even when targeted by adversarial activity. Finally, CSD drives national efforts to create a secure and resilient cyber ecosystem through the combination of a wide range of technical and non-technical capabilities. These capabilities include helping to ensure the security of software-enabled products and services, addressing gaps in the national cybersecurity workforce, and fostering innovation to make game-changing impacts in cybersecurity.

- **Emergency Communications Division (ECD):** ECD supports and promotes communications used by emergency responders and government officials to keep the United States safe, secure, and resilient. CISA leads the nation's operable and interoperable public safety and national security and emergency preparedness (NS/EP) communications efforts. The agency also provides training, coordination, tools, and guidance to help its federal, SLTT, and industry partners develop their emergency communications capabilities. CISA's programs and services coordinate emergency communications planning, preparation, and evaluation to ensure safer, better prepared communities nationwide. The emergency communications community includes the public safety community, critical infrastructure owners and operators, and any other organization that relays emergency information to its stakeholders.

III. Available Mechanisms, Programs, and Initiatives

CISA has several long-standing and recently launched outreach mechanisms, programs, and initiatives in place. This section includes information on the active national-level coordinating councils that CISA leads, convenes, or participates in, as well as the national-level, regional-level, and local-level outreach programs and initiatives led by various CISA divisions.

National-level mechanisms, programs, and initiatives (listed in the next subsection) are not specific to any state or region and may be utilized by critical infrastructure owners and operators anywhere, whereas regional and local programs are conducted through CISA's regional offices and/or its SLTT partners. While many of CISA's mechanisms, programs, and initiatives are established at the federal level and address a national-level federal government priority or policy, several of them are executed at the regional and local levels. These programs are discussed in more detail in subsequent subsections.

Available Mechanisms: National-Level Coordinating Councils

As National Coordinator and an SRMA, one of the primary mechanisms by which CISA conducts outreach and enhances public-private partnership is through convening national-level coordinating councils and collaborative groups. National-level coordinating councils bring together partners from federal and SLTT governments, regional entities, the private sector, and non-governmental organizations to collaborate on critical infrastructure security and resilience programs and approaches, and to achieve national goals and objectives. These councils provide primary organizational structures for coordinating critical infrastructure security and resilience efforts and activities within and across the 16 sectors.

Critical Infrastructure Partnership Advisory Council (CIPAC)

CIPAC was established by DHS in 2006 as a mechanism to support the sectors' interests to jointly engage in critical infrastructure discussions and to participate in a broad spectrum of activities. CIPAC forums support deliberations on critical infrastructure issues that require consensus and convene specific stakeholders to develop recommendations that are proposed to the federal government. Discussions and activities undertaken after invoking CIPAC include the following:

- Planning, coordinating, and exchanging information on sector-specific or cross-sector issues.
- Advising on operational activities related to critical infrastructure security and resilience, both in steady state and during incident response.
- Contributing to the development and implementation of national policies and plans, including this National Plan and the Sector-Specific Plans (SSPs).
- Submitting consensus advice and/or recommendations to the federal government related to critical infrastructure programs, tools, and capabilities.

Members of CIPAC include GCCs, SCCs, FSLC, CI-CSC, and SLTTGCC.

Critical Infrastructure Cross-Sector Council (CI-CSC)

CI-CSC provides a forum for Sector Coordinating Councils (SCCs) to address cross-sector issues and interdependencies. The council is composed of SCC chairs and vice chairs or their official designees. Members of CI-CSC may choose to designate or appoint a Council Chair and Vice Chair.

Government Coordinating Councils (GCCs)

GCCs enable interagency, inter-governmental, and cross-jurisdictional coordination within and across sectors. They comprise representatives from across various levels of government (i.e., federal and SLTT) to the operating landscape of each individual sector. Each GCC is chaired by a representative from the designated SRMA. The Council Chair is responsible for ensuring appropriate representation on the council and providing cross-sector coordination with SLTT governments. The GCC coordinates strategies, activities, policies, and communications across governmental entities within each sector. Reaching across the partnership, the GCC works to coordinate with and support the efforts of the SCC.

Sector Coordinating Councils (SCCs)

SCCs are self-organized, self-run, and self-governed councils that enable critical infrastructure owners and operators, trade associations, vendors, and others to interact on a wide range of sector-specific strategies, policies, activities, and issues. SCCs serve as sector policy coordination and planning entities that collaborate with SRMAs and related Government Coordinating Councils to address critical infrastructure security and resilience issues for that sector. SCCs help SRMAs fulfil their statutory responsibilities by supporting information-sharing capabilities within the sector, participating in efforts to draft the National Plan, the Sector-Specific Risk Management Plans, the corresponding Sector Risk Assessments, and supporting other activities. SCC's serve as a voice for the sector and represent principal entry points for the government to collaborate with the sector on critical infrastructure security and resilience activities. Because the SCC for each sector is self-run, each SCC has a distinct charter with unique governing principles, including how the council is chaired.

Federal Senior Leadership Council (FSLC)

FSLC serves as the primary cross-sector council for SRMAs and other federal departments and agencies responsible for critical infrastructure security and resilience. Membership in the FSLC resides with the member agency, which includes designated SRMAs and other federal departments and agencies with authorities, responsibilities, or capabilities relevant to the security and resilience of the nation's infrastructure.

NSM-22 further defined the FSLC's role in the interagency. This includes coordinating regularly with each SRMA on all sector-specific activity and regularly briefing the FSLC on cross-sector initiatives, including the sharing of best practices, data, and tools from those initiatives. The FSLC also communicates national and cross-sector guidance and priorities for SRMA efforts to the SRMAs.

Additionally, NSM-22 introduced the role of the FSLC Co-Chair. Per NSM-22, the "FSLC shall be co-chaired by the Director of CISA and a non-CISA Accountable Senior Official for an SRMA that serves a 2-year term."

Interagency Security Committee (ISC)

ISC was established to enhance the quality and effectiveness of the security in and protection of federal buildings and facilities in the United States occupied by federal employees or federal contractor workers for nonmilitary activities and to provide an ongoing entity to address continuing government-wide security for federal facilities. The committee serves as a collaborative forum that carries out its work by, with, and through its members who help guide the development of ISC policies, standards, compliance, and strategic initiatives.

The "bedrock" doctrine and standard for federal facility security is the ISC's Risk Management Process (RMP) Standard. The RMP Standard provides an integrated, single source of security countermeasures and guidance on countermeasure customization for all nonmilitary federal facilities. ISC members created the RMP Standard to do the following:

- Provide a common risk management method for all federal facility security stakeholders (i.e., owning and leasing organizations, security organizations, and members of departments and agencies that are tenants in federal facilities).
- Guide risk assessments of federal facilities in a standardized way.
- Help facility owners identify the levels of protection needed to mitigate risk.

State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC)

SLTTGCC serves as a forum to promote the engagement of SLTT partners as active participants in national critical infrastructure security and resilience efforts and to provide an organizational structure to coordinate across jurisdictions on SLTT government-level guidance, strategies, and programs.

Joint Cyber Defense Collaborative (JCDC)

JCDC was established in 2021 to drive down cyber risk to the nation by combining the visibility and insight of private sector and federal cyber ecosystem. Composed of more than 22 of

America's largest cybersecurity and technology companies, and several government agencies, JCDC provides a platform for operational collaboration and engages in an unprecedented level of public-private proactive planning. The collaborative works closely with SRMAs and the federal cyber centers.

In its short history, JCDC created a new model of persistent collaboration between industry and government to develop joint cyber defense plans and improve real-time information sharing, planning, and exercising on national threats to reduce risk. JCDC's public-private operating model strengthens lines of communication between industry and the federal government providing increased visibility into the most pressing cyber threats worldwide, turning collective insights into risk-informed action.

JCDC fulfills CISA's statutory requirements under the National Defense Authorization Act for FY 2021 to establish a Joint Cyber Planning Office (JCPO), an interagency cyber planning hub.

National Council of Statewide Interoperability Coordinators (NCSWIC)

NCSWIC supports Statewide Interoperability Coordinators (SWIC) from the 56 states and territories by developing products and services to assist them with leveraging their relationships, professional knowledge, and experience with public safety partners involved in interoperable communications at all levels of government.

CISA is the lead coordination agency for the NCSWIC and recognizes the critical role the SWICs serve in organizing and executing the interoperability effort in all the states and territories.

Available Programs and Initiatives: National-Level

CISA develops and leads outreach programs and initiatives for critical infrastructure owners and operators nationwide. These programs, tools, and trainings are not specific to any region or state, and are, therefore, intended to benefit CISA's partners and stakeholders across the country.

CISA Director's Priority Initiatives

The CISA Director's Priority Initiatives (DPIs) identify priority threat areas. DPIs align with the goals and objectives set out in CISA's Strategic Plan (2023-2025). Some DPIs are internal-focused initiatives, such as plans to grow CISA's workforce and strengthen the agency's "people first" culture. Most DPIs, however, focus on enhancing CISA's outreach mechanisms, especially to entities that lack adequate federal assistance:

- **Develop Cybersecurity Awareness Program**: This involves developing a strategy and identifying partner organizations and key influencers, such as SLTT community representatives, to champion the program's messaging.

- **Ensure Safe Elections**: This involves increasing the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) membership, enhancing the cybersecurity posture of state and local election officials, conducting cyber and protective security assessments with election infrastructure entities, training election workers, delivering tailored incident response products and security-related communications across jurisdictions, and conducting election security exercises (including a national-level election security exercise) to foster preparedness and resilience among election infrastructure stakeholders.
- **Target Rich, Resource Constrained Initiative**: Three sectors/subsectors require increased federal attention and support for their cybersecurity capabilities. This initiative involves increasing communications and engagement with the sector/subsector's stakeholders, increasing utilization of CISA services in the sector/subsector, and increasing exposure of more complex, non-scalable risk reduction services to the sector/subsector. The following sectors/subsectors are the focus of this initiative:
    - K-12 Subsector
    - Healthcare and Public Health Sector
    - Water and Wastewater Sector

Many of the programs described throughout this report align with the DPIs.

Active Shooter Preparedness Program

CISA serves as the nation's leader for active shooter preparedness within the DHS enterprise. CISA is committed to enhancing the nation's ability to prevent, protect against, mitigate, respond to, and recover from active shooter incidents. In support of critical infrastructure stakeholders, CISA delivers resources and training to enhance security and increase resilience of people, organizations, and communities, including schools, workplaces, election infrastructure sites, houses of worship, transportation centers, and other public gathering locations.

CISA provides a variety of no-cost security capacity building products, tools, and trainings to a broad range of stakeholders. These capacity building resources range from informational materials to planning-oriented tools such as templates and guides that aim to enhance security by helping organizations prepare for, respond to, and recover from active shooter incidents.

CISA conducts more than 60 virtual and in-person instructor-led training events each year, which include more than 25,000 registered participants. These events provide participants with information to proactively identify behaviors of concern, conduct effective risk assessments, implement threat management concepts to guide intervention decisions and mitigate consequences, and develop or improve active shooter emergency action plans. These events also introduce data-informed approaches to empower organizational preparedness as well as industry-informed response considerations.

CISA also offers comprehensive advice on active shooter preparedness to inform policy across the full spectrum of national preparedness mission areas including prevention, protection, mitigation, response, and recovery. CISA is positioned to deliver relevant advice through

avenues such as the DHS Center for Faith-Based and Neighborhood Partnerships and the White House Office for Gun Violence Prevention as well as through interagency mechanisms such as the Protecting Places of Worship Interagency Policy Committee (IPC) and the Targeted Violence and Terrorism Prevention Sub-IPC.

Cybersecurity Services and Assessments

CISA supports Federal, State, Local, Tribal and Territorial Governments and Critical Infrastructure partners by providing cyber scanning, testing and assessment services across a catalog of tailored options to help reduce cyber risk. The team also provides an objective third-party perspective of operational cybersecurity posture and identifies cybersecurity strengths and weaknesses. CISA turns that data into actionable reports that recommend mitigations and controls toward overall risk reduction.

Objectives of Services and Assessments:

- Reduce risk to customers
- Enable Better Informed Decision Making
- Influence Cybersecurity Best Practices
- Increase Resiliency Against Cyber Threats

Attack Surface Management (ASM)

CISA's Attack Surface Management program identifies and addresses cyber vulnerabilities in internet-facing components of networks across organizations. This is an important first step in driving down opportunities for cyber attackers to exploit critical systems.

ASM data is derived both from publicly available sources (i.e., passively gathered), as well as through active scanning from the nearly 8,700 organizations using CISA's Cyber Hygiene (CyHy) services, which include vulnerability and web scanning. These security services assist organizations in identifying and remediating specific vulnerabilities, including those listed in CISA's Known Exploited Vulnerabilities catalog. Participating organizations receive regular reporting, alerts, and mitigation recommendations so they may proactively remediate vulnerabilities and weaknesses affecting their networks. On average, CISA observes organizations reducing their vulnerable attack surfaces by 30 percent within three months of utilizing these services.

ChemLock and Chemical Security

CISA is a leader in the domestic chemical security space. In addition to its work as the Chemical SRMA, CISA offers a voluntary ChemLock program to facilities across all critical infrastructure sectors that possess dangerous chemicals. Owners and operators can access services and tools to

assist their businesses with developing and implementing chemical security plans from on-site risk assessments and tabletop exercises to guidance documents, templates, and live training.

CISA actively engages critical infrastructure owners and operators and convenes domestic and international chemical security practitioners to exchange threat information and share best practices through the Chemical Security Summit and Chemical Security Seminars and by co-implementing the Global Congress on Chemical Security and Emerging Threats.

CISA Central

CISA Central is the most centralized way for critical infrastructure partners and stakeholders, as well as regional and headquarters staff, to communicate, request assistance, share classified and unclassified information on current and emerging threats, and engage with the agency. CISA Central allows the agency to work closely with the public and private sectors, as well as international partners, coordinating the delivery of CISA's technical assistance, information security, and education to protect the nation's critical infrastructure from a broad range of cyber, communication, and physical threats. CISA Central provides 24/7 situational awareness and near-real time operational reporting.

CISA Central maintains strategic relationships with the SRMAs, most of the ISACs including Communications, Aviation, Multi-State, Elections, and Financial Services, and federal operations centers to share information with a wide range of partners.

CISA Exercises

CISA conducts cyber, physical, and emergency communications exercises with government and sector partners to enhance the security and resilience of critical infrastructure. These exercises are critical in validating plans and capabilities to address current and emerging threats and hazards and in connecting partners with available CISA resources to address identified gaps. Each year, CISA conducts a formal call for exercise requests leveraging multiple outreach mechanisms identified in this report.

CISA Gateway

CISA Gateway provides various data collection, analysis, and response tools in one integrated system through a single-user registration, management, and authentication process. Highlights of CISA Gateway include the ability to access:

- A selection of physical and cyber vulnerability assessment and security survey capabilities.
- A suite of critical infrastructure information, including assessments, analytical products, and reports.
- Integrated data visualization and mapping applications to support complex data and dependency analysis.

- An array of tools to support critical infrastructure planning and analysis, including a robust data search capability.

Counter-Improvised Explosive Devices (C-IED) and Bombing Prevention Training

CISA plays a leading role in implementing the National C-IED policy, which is articulated through Presidential Policy Directive 17: Countering Improvised Explosive Devices (IEDs). Through this leadership role, CISA is instrumental in aligning DHS and national C-IED efforts through centralized and effective coordination of ongoing programs, resulting in better resource allocation within CISA and across DHS and federal, SLTT, and private sector partners.

To reduce the risk to the nation's critical infrastructure, CISA's Office for Bombing Prevention (OBP) provides a variety of training, products, tools, and services to build nationwide C-IED core capabilities and to enhance the awareness of terrorist threats. Through these offerings, CISA OBP seeks to enhance the nation's ability to prevent, protect against, respond to, and mitigate the use of explosives against critical infrastructure, the private sector, and federal and SLTT entities. The training, products, tools, and services provided are broken into five sub-topics: bomb threats, suspicious activity and items, IED awareness, protective measures, and planning and preparedness.

The CISA Empowered Trainer Initiative is a Train-the-Trainer program designed to build C-IED training capabilities within public and private organizations by providing trainers with the essential knowledge and support required to effectively deliver OBP's C-IED and risk mitigation training in their local jurisdictions or their individual organizations using accredited curriculum and learning management systems.

CISA Technology Training Events incorporate a unique combination of industry demonstrations and experiential scenario-based training that exposes bomb disposal technicians to novel equipment and procedures and provides the opportunity to use the equipment or process under arduous simulated conditions. These events enhance individual technician capabilities and shorten product and process development feedback loops.

Critical Infrastructure Shared Services Pilot

In FY 2023, CISA received $15 million to develop a pilot program to provide scalable commercial cybersecurity shared services to critical infrastructure entities to detect and prevent cybersecurity threats and mitigate vulnerabilities more effectively. CISA has acted as a managed service provider to federal agencies for years and observed significant risk reduction along with the benefits of cost-savings and standardization. Through this pilot program, CISA is identifying critical infrastructure entities interested in leveraging CISA-provided commercial shared services, stress-testing service delivery mechanisms, and demonstrating CISA's ability to acquire, deploy, and operate these cybersecurity services at-scale. In alignment with CISA's "Target Rich, Resource Poor" strategy, CISA is working with critical infrastructure entities in the healthcare, water, and K-12 education sectors during the first phase of deployment.

The first year of the program culminated with the roll out of the initial service offering, Protective Domain Name System (DNS), which is a specialized firewall that uses federal and commercial threat intelligence to prevent systems from connecting to known or suspected malicious domains. The service is fully operational and continuing to onboard critical infrastructure organizations utilizing pilot funding. As of June 2024, 63 organizations are routing traffic through this service, which has prevented over 4.5 million malicious DNS connections.

Cybersecurity Awareness Month

In 2004, the President of the United States and Congress declared the month of October to be Cybersecurity Awareness Month, a dedicated month for the public and private sectors to work together to raise awareness about the importance of cybersecurity. Over the years it has grown into a collaborative effort between government and industry to enhance cybersecurity awareness, to encourage the public to take actions to reduce online risk, and to generate discussion on cyber threats on a national and global scale. October 2023 marked the 20th Cybersecurity Awareness Month. Starting in 2023 with the launch of a new cybersecurity awareness program, "Secure Our World," described in more detail below, will be the enduring theme for all future Cybersecurity Awareness Months. Organizations can use the "Secure Our World" theme as they plan for the 2024 and future Cybersecurity Awareness Month campaigns.

CyberSentry

CyberSentry is a CISA-managed threat detection and monitoring capability that provides operational visibility into information technology and operational technology (IT/OT) networks within participating critical infrastructure entities. CyberSentry monitors for malicious activity affecting critical infrastructure participants' IT/OT networks, in many cases using sensitive information derived from government or international partners. If malicious activity is identified on the partner's network, CISA notifies the partner to confirm the activity. If the partner confirms the activity as malicious, CISA analysts will share recommended actions; however, it is a partner's responsibility to implement any recommendations. CISA is able to provide technical assistance to a partner upon request, and availability of resources.

Nearly 30 companies are now participating in CyberSentry, including major oil and natural gas pipelines, energy generation facilities, large airports, and critical manufacturing facilities. CISA is working with critical stakeholders, such as CISA's NRMC and various SRMAs, enhancements to onboarding and threat reduction.

The Emergency Communications Preparedness Center (ECPC)

Administered by CISA, ECPC is the federal interagency focal point for interoperable communications coordination. It is currently comprised of 14 departments and agencies who represent the federal government's broad role in emergency communications including regulation, policy, operations, grants, and technical assistance. Current members are the Federal Communications Commission, the General Services Administration, and the U.S. Departments of Agriculture, Commerce, Defense, Energy, Health and Human Services, Homeland Security, Interior, Justice, Labor, State, Transportation, and Treasury.

Emergency Communications Coordination Program

CISA supports and promotes the nationwide improvement of emergency communications capabilities through the Emergency Communications Coordination Program. CISA has subject matter experts located across the country to engage stakeholders and address complex issues facing the emergency communications ecosystem. These Emergency Communications Coordinators build trusted relationships, enhance collaboration, and share best practices and information between all levels of government, critical infrastructure owners and operators, and key non-governmental organizations. Emergency Communications Coordinators seek to build partnerships between federal and SLTT government stakeholders as well as the private sector. These partnerships result in a united effort to improve the nation's operable and interoperable emergency communications.

Federal Partnership for Interoperable Communications (FPIC)

FPIC serves as a coordination and advisory body to address technical and operational wireless issues relative to interoperability within the public safety emergency communications community, interfacing with voluntary representatives from federal and SLTT organizations.

Federal School Safety Clearinghouse and SchoolSafety.gov

On behalf of the U.S. Departments of Education, Health and Human Services, Homeland Security, and Justice, CISA administers and manages the Federal School Safety Clearinghouse (Clearinghouse) and its public-facing website, SchoolSafety.gov. The Clearinghouse serves as an ongoing and coordinated effort that includes regular interagency review of evidence-based content and recommended best practices to keep schools safe as well as the curation and distribution of resources, guidance, and tools for school communities across the country. SchoolSafety.gov is a collaborative, interagency website to provide schools and districts with actionable recommendations to create safe and supportive environments for students and educators. The site serves as a one-stop access point for the American public and school communities to find information, resources, guidance, and evidence-based practices on a range of school safety topics.

Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force

Co-chaired by CISA and the Information Technology and Communications Sector Coordinating Councils, the ICT SCRM Task Force is a public-private partnership charged to identify, develop, and promote consensus risk management strategies to enhance global ICT supply chain security. It serves as the agency's center of gravity for supply chain risk management partnership activity.

National Emergency Communications Plan (NECP)

The NECP is the nation's strategic plan to strengthen and enhance emergency communications capabilities. It establishes a shared vision for emergency communications and assists those who plan for, coordinate, invest in, and use operable and interoperable communications for response and recovery operations. CISA is currently updating the NECP and is conducting outreach across the whole community (e.g., traditional emergency responder disciplines and other partners that share information during incidents and planned events) to seek their input to the NECP. In particular ECD, in collaboration with SED, has initiated a targeted outreach to the critical infrastructure sectors to enhance their understanding of their role in emergency communications, build partnerships, and obtain their input on the NECP to ensure its vision truly is reflective of the whole community.

National Summit on K-12 School Safety and Security

CISA plays a critical role in supporting the federal government's efforts toward strengthening the safety and security of kindergarten through grade 12 (K-12) schools across the country. CISA hosts the annual National Summit on K-12 School Safety and Security, which brings federal and SLTT school leaders together to share actionable recommendations that enhance safe and supportive learning environments in K-12 schools. Through expert panels and keynote addresses by leaders in the field, the summit explores current threats and issues in school safety and considers research-informed strategies for addressing security challenges. The summit aims to support the safety and security of the nation's schools by fostering a nationwide dialogue by bringing together stakeholders for exchange, discussion, and connection; facilitating action by sharing resources, products, and tools to support schools in implementing and strengthening their security postures; and equipping stakeholders with training and expertise to apply recognized best practices and research in the context of their specific communities, venues, and schools.

Protect2024

Protect2024 is CISA's campaign to help election officials and election infrastructure stakeholders protect against cyber, physical, and operational security risks to election infrastructure during the 2024 election cycle. CISA's Protect2024 mission is coordinated nationally at the headquarters level but is executed at the regional level. CISA Election Security

Advisors are deployed across the 10 Regions to work closely with state election offices and local election officials to help guide and shape support to meet unique state, local, and private-sector election infrastructure stakeholder requirements. Voluntary, no-cost election security training is available from CISA on demand as well as Tabletop the Vote, CISA's yearly national election security exercise that provides an opportunity for federal partners, state and local election officials, and vendors to identify and share best practices and areas for improvement related to election security.

Protected Critical Infrastructure Information (PCII) Program

The PCII Program, created by the Critical Infrastructure Information Act of 2002 and implemented in Title 6 of the Code of Federal Regulations part 29, "Protected Critical Infrastructure Information," establishes uniform procedures on the receipt, validation, handling, storage, marking, and use of cyber and physical critical infrastructure information (CII) voluntarily submitted to CISA. The protections offered by the PCII Program enhance the voluntary sharing of CII between private/SLTT infrastructure owners and operators and the government. The PCII Program protects information from public disclosure while allowing DHS/CISA and other federal, state, and local government security analysts to:

- Analyze and secure critical infrastructure and protected systems.
- Identify vulnerabilities and develop risk assessments.
- Enhance preparedness, resilience, and recovery measures.

Resilience Planning Program

Through the Resilience Planning Program, CISA collaborates with infrastructure stakeholders at all levels to create solutions that enhance critical infrastructure security and resilience. The Resilience Planning Program offers an interdisciplinary and partnership-based approach that incorporates resilience strategies and policies into all phases of critical infrastructure planning, design, construction, and maintenance. This holistic approach helps public and private owners and operators, as well as SLTT planners and policy makers, effectively prioritize and integrate resilience measures into policies, plans, designs, and operational procedures.

SAFECOM

Through collaboration with emergency responders and elected officials across all levels of government, SAFECOM works to improve emergency response providers' inter-jurisdictional and interdisciplinary emergency communications interoperability across SLTT and international borders, and with federal government entities. SAFECOM works with existing federal communications programs and key emergency response stakeholders to address the need to develop better technologies and processes for the coordination of existing communications systems and future networks.

School Safety and Security

In addition to the National Summit on K-12 School Safety and Security mentioned above, CISA's ongoing school safety efforts include the development of new programs and capacity building products, training, and tools specific to strengthening protection and mitigation measures and capabilities at K-12 schools. CISA's resources and programs are designed to help schools prevent, protect against, and mitigate security threats, risks, and emergency situations.

Specific efforts include the K-12 School Security Guide Product Suite, which is designed to provide K-12 districts and campuses with resources, tools, and strategies to improve school physical security. In addition, CISA released the K-12 Bystander Reporting Toolkit, which supports K-12 schools and districts in strengthening school safety reporting programs and encouraging bystander reporting among students and other members of the school community. Developed in partnership with the U.S. Secret Service National Threat Assessment Center, the toolkit offers simple strategies and guidance to implement or enhance safety reporting programs and create a school environment where students are more willing and able to report concerns for the wellness and safety of themselves or others. CISA also regularly communicates with the K-12 academic community and other relevant school safety stakeholders. By leveraging current events and topics, the School Safety Task Force raises awareness of school safety-related tools, resources, and guides, and educates school communities on current and emerging threats and hazards.

Secure Our World

CISA's Secure Our World program launched on September 26, 2023, and encourages individuals, families, and small and medium-sized business owners to take four simple steps: use strong passwords; install automatic updates; enable multi-factor authentication; and recognize and report phishing to stay safe and secure online. The program is enduring, and there are many ready-made tools developed for the program such as two public service announcements that are available on cisa.gov.

Securing Public Gatherings and Houses of Worship Programs

CISA plays a critical role in advancing the security of critical infrastructure facilities that provide for large public gatherings. Through a comprehensive set of programs that build public and private sector security capacity to mitigate a wide range of risks, CISA helps secure these facilities from threats through the development and delivery of innovative solutions. In addition to direct support provided by Protective Security Advisors (PSAs) and threat-specific and general security trainings and exercises, CISA also provides a multitude of capabilities through its Securing Public Gatherings website. The capabilities shared include conflict prevention techniques which enable organizations to mitigate potentially escalating situations through purposeful and safe actions.

As part of the public gathering security effort, and due to the prevalence of incidents and threats, CISA places particular emphasis on advancing the security of houses of worship. The agency focuses on addressing terrorism and targeted violence threats, while sustaining the necessary open and welcoming environment, through a multitude of resources which are frequently accessed by the public. For example, the Protecting Houses of Worship website was viewed by stakeholders more than 100,000 times in FY 2023. Additionally, a self-assessment tool developed specifically for faith-based leaders to easily determine potential security gaps and help inform investments was utilized more than 60,000 times. In December 2023, CISA released the Physical Security Performance Goals for Faith-Based Communities to provide a set of baseline security best practices that assist houses of worship and related facilities to reduce risk through tangible security measures that are scalable depending on existing security protocols and available funding. This document also directly responds to requests from faith-based partners to provide a single resource of consolidated, easily consumable security recommendations.

SRMA Coordination Conference Call

The monthly SRMA coordination conference call provides regular communication and coordination among representatives from the SRMAs and other federal departments and agencies with responsibility for critical infrastructure security and resilience activities.

The SRMA coordination conference call coordinates important work and amplifies messaging on efforts such as Executive Orders (EO), including AI EO 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (AI EO); CISA's work, such as Cybersecurity Performance Goals and Sector-Specific Cybersecurity Performance Goals, the Joint Ransomware Task Force, and the National Critical Infrastructure Prioritization Program; and National Security Memoranda (NSM), such as NSM-5: Improving Cybersecurity for Critical Infrastructure Control Systems and NSM-22.

Through a collaborative, iterative, and transparent process, and with the help of SRMAs, the call successfully compiled important feedback on key deliverables, such as AI EO Section 4.3(a)(iii); Private Sector Key Intelligence Questions, solicited annually; Sector Risk Assessments, released periodically on a wide range of topics; National Cyber Incident Response Plan; and Common Baseline for the Cybersecurity Performance Goals.

Stakeholder Relationship Management (SRM) Tool

The SRM program and information technology tool supports CISA's mission to lead the national effort to understand and manage cyber and physical risk to the nation's critical infrastructure. The SRM program provides stakeholders with necessary knowledge in a streamlined and effective way and ensures a consistent and coordinated stakeholder engagement approach. This program provides a comprehensive picture of CISA's stakeholders, including how and when CISA engages them, how stakeholders access and use CISA products and services, and where CISA should focus its outreach and engagement efforts to deliver its products and services more efficiently.

Achieving full operational capability of the SRM tool across CISA is essential to ensuring that CISA can harvest detailed, centralized, and authoritative knowledge of stakeholders, their interests and key equities, and the scope of their integration with the broader national critical infrastructure stakeholder community. These specifics are necessary to effectively collaborate and build more secure and resilient infrastructure.

Technical Resource for Incident Prevention (TRIPwire)

TRIPwire is CISA's cross-cutting foundational resource for the integration, analysis, and visualization of IED incidents and C-IED capability data to increase the awareness of evolving terrorist IED tactics, techniques, and procedures, as well as lessons learned from incidents and information on C-IED preparedness. This resource creates a cohesive national C-IED Common Operating Picture to more effectively identify and address IED incidents and C-IED capability gaps. Through these efforts, TRIPwire enhances the delivery of C-IED resources and capabilities to the nation's security and emergency services professionals. The portal currently supports 10,565 registered users across all 50 states and the territories and 60,000 unique visitors annually.

Available Programs and Initiatives: Regional Level

While many of CISA's programs are established at the federal level and are applicable to partners nationwide, CISA conducts several of them regionally and locally.

CISA's regional offices communicate with owners and operators of critical infrastructure. This agency-wide approach will aim to address any limitations in the current level of cooperation among critical infrastructure owners and operators.

CISA delivers services to regional stakeholders through its 10 regional offices. These offices provide a range of cyber and physical services to support the security and resilience of critical infrastructure owners and operators, as well as SLTT partners, throughout the country. Through these offices, regional personnel carry out steady state and incident operations, critical infrastructure analysis, and strategic outreach to critical infrastructure partners. Chemical Security Inspectors, Cybersecurity Advisors, Emergency Communications Coordinators, Election Security Advisors, and Protective Security Advisors all coordinate critical infrastructure protection missions. The CISA regional offices align with the 10 Federal Emergency Management Agency (FEMA) regions.

- **Chemical Security Inspectors (CSIs)**: CSIs safeguard the American people by preventing the misuse of chemicals in a terrorist attack on the homeland. Every day, thousands of chemical facilities across the country—from small companies to national laboratories—use, manufacture, store, and transport dangerous chemicals in a complex, global chain that affects other critical infrastructure sectors. CSIs manage programs such

as ChemLock 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.

- **Cybersecurity Advisors (CSAs):** CSAs 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.
- **Election Security Advisors (ESAs)**: ESAs are subject matter experts in state and local elections processes, procedures, and technologies. As members of CISA's regional teams, ESAs use their in-depth understanding of election administration processes and risks to election infrastructure to help ensure that state and local election officials on the front lines of defending the elections process receive the most effective physical security and cybersecurity assessments, services, and trainings to meet their unique jurisdictional requirements. ESAs are part of CISA's regional teams, working directly with CSAs and PSAs to ensure CISA's capabilities and services are being optimally employed to meet the specific needs of each state or locality. ESAs increase the agency's internal election security expertise, augment its ability to coordinate efforts to support elections stakeholders, and ensure CISA is providing the most effective risk mitigation assistance possible.
- **Emergency Communication Coordinators (ECCs)**: ECCs support emergency communications interoperability by offering training, tools, and workshops, and provide coordination and support in times of threat, disruption, or attack. These services assist CISA stakeholders in ensuring they have communications during steady and emergency operations. Through these programs, CISA helps ensure public safety and national security and emergency preparedness communities can seamlessly and securely communicate.
- **Protective Security Advisors (PSAs)**: PSAs are 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 SLTT officials and critical infrastructure owners and operators and provide coordination and support in times of threat, disruption, or attack.

Listed below are regional-level initiatives and programs that CISA has in place.

CISA Regional Service Delivery

With Regional Service Delivery, CISA is improving the delivery of products and services to critical infrastructure owners and operators and SLTT partners and enhancing support to existing CISA regional staff by relocating administrative, logistical, and regional operations capabilities from CISA Headquarters to 10 regional offices. By the end of FY 2024, CISA will standardize CISA Regional Service Delivery and its product rollout across the 10 CISA Regions.

Pre-Ransomware Notification Initiative (PRNI)

Through the PRNI, CISA uses tips from researchers and industry to notify organizations of a ransomware compromise prior to the actorencypting or stealing data. By notifying these entities, they can often implement a remediation before damage occurs. In 2023, CISA conducted over 1,200 Pre-Ransomware Notifications, including hundreds of K-12 school districts, SLTT government entities, healthcare organizations, and hospitals. Also, 294 pre-ransomware notifications were shared with 27 partner countries.

Ransomware Vulnerability Warning Pilot (RVWP)

As part of the RVWP, CISA leverages existing authorities and technology to proactively identify information systems that contain security vulnerabilities commonly associated with ransomware attacks. Once CISA identifies these affected systems, regional cybersecurity personnel notify system owners of their security vulnerabilities, thereby enabling timely mitigation before damaging intrusions occur. In 2023, CSD conducted over 1,700 notifications to organizations including hospitals, water utilities, K-12 school districts, and election jurisdictions about open vulnerabilities on their networks.

Regional Resilience Assessment Program (RRAP)

The RRAP is a voluntary, cooperative assessment of specific critical infrastructure that identifies a range of security and resilience issues that could have regionally or nationally significant consequences. The goal of the RRAP is to generate understanding and action among public and private sector partners to improve the resilience of a region's critical infrastructure. Strong partnerships with federal and SLTT government officials and private sector organizations across multiple disciplines are essential to the RRAP process. This includes private sector facility owners and operators, industry organizations, emergency response and recovery organizations, utility providers, transportation agencies and authorities, planning commissions, law enforcement, academic institutions, and research centers.

Each RRAP project typically involves a year-long process to collect and analyze information on the critical infrastructure within the designated area, followed by continued technical assistance to enhance the infrastructure's resilience. Individual projects can incorporate many different analytic activities and opportunities for valuable information to improve security and resilience efforts. Multiple RRAP projects are currently ongoing and CISA will initiate one new RRAP project in 2025.

Southwest Border Communications Working Group (SWBCWG)

As part of its role to assist federal and SLTT agencies in establishing and maintaining interoperable emergency communications, CISA coordinates the activities of SWBCWG.

SWBCWG serves as a forum for federal and SLTT agencies in Arizona, California, New Mexico, and Texas to share information about common communications issues; collaborate on existing and planned activities; and facilitate federal involvement in multi-agency projects within the Southwest Border Region. SWBCWG aims to enhance communications operability and interoperability, effectively use the regions available critical communications infrastructure resources, and ensure that programs continue to meet stakeholders' needs.

SWBCWG participants include representatives from 10 federal offices, 20 state agencies, 66 local agencies and six tribal nations who rely on communications to support critical public safety and border security missions. Participants include stakeholders from various disciplines, including system managers; communications engineers and technicians; spectrum managers; emergency managers and planners; federal, state, and local law enforcement; and fire and emergency medical services officials and practitioners.

Available Programs and Initiatives: Local Level

This section includes an overview of programs and initiatives focused on primarily benefitting CISA's SLTT partners and stakeholders.

Connected Communities Initiative (CCI)

Connected Communities are communities (e.g., rural, suburban, and urban) that leverage networks of connected technologies to provide more efficient, innovative, and sustainable infrastructure across the nation.

CCI represents a shift in CISA's focus from exclusively supporting the security and resilience of 5G networks to the comprehensive examination of the technologies that those networks are intended to enable. Integrating a greater number of previously separate infrastructure systems into a single network environment expands the digital attack surface, increasing opportunities for threat actors to successfully exploit a vulnerability for initial access, move laterally across networks, and cause cascading, cross-sector disruptions of infrastructure operations. The possible impacts due to these risks have prompted CISA to establish the CCI to develop, organize, and coordinate risk mitigation strategies relating to smart and connected technologies. CISA conducts outreach in coordination with a newly formed CCI working group.

Last Mile Initiative

Thousands of local jurisdictions make up the U.S. elections stakeholder community and together represent the "Last Mile" in reducing risk to election infrastructure. The CISA Last Mile initiative provides election administrators and their partners a range of customizable resources based on security best practices and industry standards to help secure election infrastructure nationwide.

Last Mile products range from informational posters to lanyard cards and can be tailored to meet the unique needs of state and local election administrators and the private-sector partners that support them. Final products are the result of active collaboration between CISA and the customer to address dynamic or conditional cyber and infrastructure risks.

Multi-State Information Sharing and Analysis Center (MS-ISAC)

The MS-ISAC is a CISA-supported collaboration with the Center for Internet Security designed to serve as the central cybersecurity resource for the nation's SLTT governments. The MS-ISAC is a membership-based collaborative open to SLTT entities of all types including but not limited to: SLTT government agencies, law enforcement, educational institutions, public utilities, and transportation authorities.

MS-ISAC members receive direct access to a suite of services and informational products including cybersecurity advisories and alerts, vulnerability assessments, incident response support, secure information sharing, tabletop exercises, a weekly malicious domains/Internet Protocol (IP) report, and more.

Rural Emergency Communications Operational Rapid Assistance Package (O-RAP)

O-RAP is a technical assistance program assisting rural communities by examining communications barriers and identifying solutions that enhance existing emergency communications infrastructure to improve the delivery of rural medical care. The program is designed for county and local public safety agencies in rural communications and offered by CISA's Interoperable Communications Technical Assistance Program (ICTAP). ICTAP serves all 50 states and the territories, as well as 574 tribes, and provides direct support to emergency responders and government officials through the development and delivery of training, tools, and onsite assistance to advance public safety interoperable communications capabilities.

State and Local Cybersecurity Grant Program (SLCGP)

The SLCGP is a first-of-its-kind cybersecurity grant program specifically for SLTT governments across the country. Funding from the SLCGP and the Tribal Cybersecurity Grant Program (TCGP) helps eligible entities address cybersecurity risks and threats to information systems owned or operated by—or on behalf of—SLTT governments. Through two distinct Notices of Funding Opportunity, SLCGP and TCGP combined will make available $1 billion over four years to support projects throughout the performance period of up to four years, including $200 million in FY 2022 and $400 million in FY 2023.

Tribal Cybersecurity Grant Program (TCGP)

In September 2023, DHS announced the TCGP, which provides approximately $18.2 million to address cybersecurity risks and threats to information systems owned or operated by tribal governments in FY 2023. The TCGP will help tribal governments address cybersecurity risks and threats to their information systems by enabling DHS to provide targeted cybersecurity resources that improve the security of critical infrastructure and resilience of the services that tribal governments provide to their members.

CISA and FEMA are jointly managing the SLCGP and TCGP. CISA will provide cybersecurity programmatic subject-matter expertise by defining goals and objectives, reviewing and approving cybersecurity plans establishing measures of effectiveness, and organizing Objective Review Panels to review and score applications. FEMA will provide administrative guidance through conducting eligibility reviews and administering grant awards consistent with all applicable laws, regulations, and policies.

IV. Level of Critical Infrastructure Sector Cooperation

Critical infrastructure security is a shared responsibility between federal and SLTT governments, public and private owners and operators, and other stakeholders. Public-private collaboration is essential, including a robust information sharing environment.

Collaboration and strong partnerships are one of CISA's core values and essential to executing its mission. As noted throughout this document, CISA has a number of mechanisms, programs, and initiatives to foster and support critical infrastructure cooperation. For example, every sector has an SCC and GCC. Recently, CISA embarked on an incredible period of cooperation and coordination as part of the SRMA designation process, where stakeholders from across sectors were engaged and provided input and insights.

CISA is in the process of executing National Security Memorandum (NSM)-22 requirements, including those supporting sector cooperation, ensuring engagements are coordinated across partners and enabling effective information sharing and outreach. One of the NSM-22 requirements is developing the 2025 National Plan that will articulate how the federal government will collaborate with partners to identify and manage risk. The National Plan will replace the 2013 National Infrastructure Protection Plan, and its development and execution will rely on collaboration and cooperation with federal, SLTT, and private sector partners.

V. Gaps and Potential Overlap in Outreach Mechanisms

Between 2019 and 2023, the eight CISA SRMA sectors, GCCs and SCCs sought to identify sector security and resilience needs that could be addressed under the 2013 National Infrastructure Protection Plan framework. The information gathered from the private sector during this process will provide foundational information for the development of the Sector Risk Management Plans, as required by NSM-22.

While each sector has specific needs and challenges, there are certain cross-sector gaps and limitations related to critical infrastructure outreach, including the need to improve information sharing and knowledge coordination. Not all outreach gaps are addressed below, focusing on those from the eight CISA SRMA sectors, but those discussed below serve as a foundation to address potential gaps and limitations within other outreach topics and initiatives.

Information Sharing

Information sharing is an essential component of outreach, especially with government and private and public stakeholders involved. There is a need to identify barriers to information sharing between CISA and the private sector and enact remedial strategies.

Sectors recognize the need for restrictions on classified information and information sharing, but such restrictions can inhibit the ability to respond quickly and efficiently to incidents. To address these limitations, the sectors suggest:

- Allowing sector stakeholders access to more information by adjusting the security classification of some information.
- Creating a sharing mechanism or leveraging an existing capability (e.g., DHS's Homeland Security Information Network) where the federal government can share sanitized intelligence that sector stakeholders can access as soon as threat information is available.
- Shortening the time to downgrade classified information to provide actionable intelligence for the sectors.

Multiple sectors identified information sharing in general, not just classified information, as a challenge, specifically preemptive information on emerging threats, vulnerabilities, and criminal activity. Real-time information sharing, as well as guidelines for sharing information, is needed between sectors, critical infrastructure stakeholders, and federal, state, and local governments not only during incidents but before they occur. Possible avenues to address challenges in information sharing include:

- Developing a platform for cross-sector information sharing so that sector members have access to timely, distilled, and actionable insight into sector disruptions or threats.
- Creating a cross-sector information sharing working group to share ideas across sectors to share solutions and develop common strategies for risk mitigation.

- Investigating methods to improve regional information sharing, collaboration, and coordination within the sectors and with other critical infrastructure organizations in the region.
- Identifying existing hubs for intelligence analysis and near-real time sharing and, as appropriate and necessary, partner with federal agencies and across sectors to access or develop a central hub for intelligence analysis and near-real time sharing of infrastructure threats.

Engagement, Communication, and Coordination

Engagement between sector stakeholders and the federal government, particularly CISA, is needed to identify sector-wide pre-threat information and help prepare for and mitigate potential incidents. Increased interagency, cross-sector, and interdisciplinary engagement, coordination, and communication is required across the sectors to enhance best practices, improve awareness and communication of sector stakeholders, and increase information sharing. Consistent, up-to-date information keeps sector stakeholders informed while reducing risks and threats. Some possibilities to improve engagement and coordination within critical infrastructure sectors and with state and federal government include:

- Establishing a communication and tracking network that includes stakeholders across critical infrastructure sectors to help to better identify and monitor critical sector interdependencies.
- Conducting multi-sector activities (e.g., meetings, exercises) to build awareness and test actions of cross-cutting threats and vulnerabilities associated with dependencies and interdependencies.
- Identifying methods for routine and more frequent analytic exchanges (i.e., briefings with discussion) between the private sector and government to better prepare for risks and understand the physical and cyber threat environment.
- Identifying and developing guidance on common credentialing and access needs for both workers and equipment to support pre-crisis coordination practices and recommendations to support continuity of operations for sectors during a crisis.
- Exploring the development of a memorandum of understanding template for nationwide use that includes example language for improving methods of communication and collaboration between federal and state agencies.
- Enlisting additional PSAs to establish comprehensive reviews for the private sector.

2024 CISA Activities that Address Outreach Gaps

This table highlights current activities CISA is pursuing across its divisions to address the outreach gaps and limitations, including those mentioned by the sectors. These activities are under way or will be initiated, deployed, or expanded by the end of FY 2024. This table does not

include all CISA and DHS outreach activities but focuses on those gaps and initiatives addressed most recently by the eight CISA SRMA sectors.

Table 1: Outreach Activities to be Completed by End of FY 2024 by CISA Division

CISA Division or Office	Outreach Activity to be Completed by End of FY 2024	Description
Stakeholder Engagement Division (SED)	Utilize SRM Program to Enhance Communication	CISA will continue to utilize the SRM Program to enhance communication and awareness between CISA's Sector Liaisons and other CISA Sector Management Branches concerning requests, engagements, services delivered, and SRMA feedback.
	Document SRMA Information Sharing Gaps	CISA is currently documenting all SRMA information sharing gaps and will assist SRMAs to develop a process to mature their capabilities.
	Identify and Execute a CISA-Owned Awareness and Outreach Brand	Identify, create, and execute a CISA-owned and trademarked "Awareness and Outreach" brand to enhance the agency's mission and achieve CISA brand recognition.
	Engage with Sector Working Groups and Councils on Artificial Intelligence (AI) Adoption	CISA will engage with sector working groups and councils to determine security and resilience challenges of AI adoption.
Cybersecurity Division (CSD)	Establish Mechanisms to Measure Operational Partner Engagement	In 2024, CISA will establish consistent and repeatable mechanisms to measure operational partner engagement, provide feedback to partners regarding engagement levels, and develop workplans to improve engagement where appropriate.
	Launch New .Gov Registry	CISA will launch the new .gov registry and registrar to improve customer experience and enhance adoption by SLTT governments.
Emergency Communications Division (ECD)	Offer Technical Assistance (TA) for SLTT Partners in Priority Sectors	During 2024, CISA will develop and offer additional emergency communications interoperability and resilience TA for SLTT partners in the K-12, water and wastewater, healthcare, and election security sectors.
	Provide national metrics for emergency communications resilience ratings	Annually, CISA gathers emergency communications resilience ratings based upon a 25-question markers program. The results are self-reported by the Statewide Interoperability Coordinators.
	Identify Opportunities to Engage with Emergency Communications Associations	CISA will identify and prioritize opportunities to participate and engage emergency communications associations to enhance coordination with existing stakeholders that support identification and verification of vulnerabilities.

CISA Division or Office	Outreach Activity to be Completed by End of FY 2024	Description
Infrastructure Security Division (ISD)	Provide Security and Resilience Training to SLTT Entities	CISA is increasing awareness and capacity for infrastructure security and resilience through trainings focused on SLTT stakeholders.
	Technical Assistance Program	CISA will strengthen C-IED interagency collaboration and stakeholder engagement with federal government entities, state agencies, local jurisdictions, and the private sector. Additionally, CISA is facilitating active stakeholder involvement, ensuring robust collaborative partnerships, and enhancing community procedural and technical capabilities to effectively manage IED incidents at strategic, operational, and tactical levels.
	Develop Crowded Spaces and Soft Targets Awareness/Training	CISA is developing 11 workshops to increase awareness and training about threats to critical infrastructure with crowded spaces and soft targets.
	Conduct Federal Facility Security Training and TA Sessions	By the end of FY 2024, CISA will conduct 50 TA or Compliance Assistance sessions to federal facility partners across the CISA Regions to ensure awareness of and compliance with the Interagency Security Committee Risk Management Process.
	Incident Use Tool Training – Special Events and Domestic Incidents Tracker	CISA is in the process of conducting advanced training for planning and operations before, during, and after an incident through the Special Events/Domestic Incidents Tracker tool.
	Execute Bomb-making Materials Awareness Program (BMAP) Nationwide	CISA plans to execute BMAP nationwide by engaging with commercial organizations, including at least one corporate-level retail organization and 4,200 point-of-sale outreach at businesses that sell and distribute products containing explosive precursor chemicals.
	Coordinate with DHS Countering Weapons of Mass Destruction (CWMD) Office on AI-Driven Threats to Biosecurity and Biodefense	CISA is coordinating with the DHS CWMD Office and other relevant DHS components to ensure appropriate information sharing on AI-driven threats to biosecurity and biodefense.
National Risk Management Center (NRMC)	Execute the Technology Development and Deployment Program (TDDP) to support RRAP requirements	CISA is working to execute the TDDP to support requirements from the RRAP process. This will ensure that CISA is using research and development funding to support its external partners.
	Hold an ICT SCRM Task Force Conference	CISA is planning to hold an ICT SCRM Task Force conference to enhance information sharing efforts with its partnership base.

CISA Division or Office	Outreach Activity to be Completed by End of FY 2024	Description
	Initiate SLTT Strategic Engagement on Election Infrastructure Security	CISA conducts strategic engagement opportunities to enhance security and understanding of election infrastructure for SLTT partners.
	Assist Election Infrastructure Stakeholders in Understanding Foreign Influence and Disinformation Risks	CISA assists election infrastructure stakeholders in understanding foreign influence and disinformation risks.
Integrated Operations Division (IOD)	Integrate CISA Central with all CISA divisions and offices.	To meet the Strategic Planning Initiative making CISA Central the agency's premier Operations Center, IOD will integrate CISA Central with CISA divisions and offices.
	Provide Threat Intelligence to appropriate Election Staff with emphasis on New Election Officials.	CISA will work with election staff at state, local, tribal, and territorial levels to provide unclassified and classified election threat intelligence.
	Provide Technical Assistance to State/Local Officials on the Cybersecurity Grant Program Activities	Provide technical assistance to state and local officials regarding the Cybersecurity Grant Program and activities.
	Provide CISA Services to Enhance Resiliency through Engagement with Priority Sectors	CISA field staff will provide CISA Services in support of the CISA DPIs for FY 2024 to enhance resiliency in priority sectors to include the Department of Health and Human Services, Health ISAC, and the Health Sector Coordinating Council.
	Provide Statewide Interoperable Communications Plans (SCIP) to states.	Every 3 to 5 years, CISA will provide a SCIP workshop and plan to each state.
	Include Products and Services Related to Incorporating AI into CISA Service Delivery	Standardize CISA Service Delivery and product rollout across the 10 CISA Regions to include new products and services related to or incorporating AI.
Office of the Chief External Affairs Officer	Launch K-12 Communications Campaign	In 2024, CISA will launch a K-12 communications campaign with additional regional and sector-specific speaking and media engagements as part of the CISA Director's "Target Rich, Resource Poor" initiative.
	Launch Healthcare Sector Campaign with the Department of Health and Human Services (HHS)	During 2024, CISA will launch a healthcare sector campaign in collaboration with HHS. This will include national and regional speaking and media engagements, digital outreach, and a new campaign page on CISA.gov.

CISA Division or Office	Outreach Activity to be Completed by End of FY 2024	Description
	Launch Water Sector Campaign with the Environmental Protection Agency (EPA)	In 2024, CISA will launch a water sector campaign in collaboration with EPA. This campaign will include national and regional speaking engagements, digital outreach, and a new campaign page on CISA.gov.
	Execute an Election Security Communications Campaign	Continue to build and execute a communications campaign that reaches the election community.

Potential Overlap in Outreach Mechanisms

The expansive and comprehensive model that CISA employs to ensure effective partnership across both government and the private sector alike will, by design, include some degree of overlap both nationally and regionally. This overlap is a necessary feature of the model to ensure that CISA can communicate and engage effectively and that partners receive and provide timely and actionable information. Through careful internal coordination of mission delivery across CISA divisions, the agency can reduce this overlap to the useful minimum while still providing effective coverage across an extensive array of stakeholders.

VI. Appendix: Abbreviations

Abbreviation	Definition
CCI	Connected Communities Initiative
CI-CSC	Critical Infrastructure Cross-Sector Council
C-IED	Counter-Improvised Explosive Devices
CII	Critical Infrastructure Information
CIPAC	Critical Infrastructure Partnership Advisory Council
CISA	Cybersecurity and Infrastructure Security Agency
CSA	Cybersecurity Advisor
CSD	Cybersecurity Division
CSI	Chemical Security Inspector
DNS	Protective Domain Name System
DPI	Director's Priority Initiatives
ECC	Emergency Communications Coordinator r
ECD	Emergency Communications Division
ECPC	Emergency Communications Preparedness Center
EI-ISAC	Election Infrastructure Information Sharing and Analysis Center
EPA	Environmental Protection Agency
ESA	Election Security Advisor
FPIC	Federal Partnership for Interoperable Communications
FSLC	Federal Senior Leadership Council
GCC	Government Coordinating Council
HHS	Health and Human Services
ICT	Information and Communications Technology
IOD	Integrated Operations Division
ISC	Interagency Security Committee
ISD	Infrastructure Security Division
JCDC	Joint Cyber Defense Collaborative
MS-ISAC	Multi-State Information and Analysis Center
NCSWIC	National Council of Statewide Interoperability Coordinators
NECP	National Emergency Communications Plan
NRMC	National Risk Management Center
OBP	Office for Bombing Prevention
O-RAP	Operational Rapid Assistance Package
PCII	Protected Critical Infrastructure Information
PRNI	Pre-Ransomware Notification Initiative
PSA	Protective Security Advisor
RRAP	Regional Resilience Assessment Program
RVWP	Ransomware Vulnerability Warning Pilot
SCC	Sector Coordinating Council
SCIP	Statewide Interoperable Communications Plans
SCRM	Supply Chain Risk Management

Abbreviation	Definition
SED	Stakeholder Engagement Division
SLCGP	State and Local Cybersecurity Grant Program
SLTT	State, Local, Tribal, and Territorial
SRM	Stakeholder Relationship Management
SRMA	Sector Risk Management Agency
SSP	Sector-Specific Plans
SWBCWG	Southwest Border Communications Working Group
SWIC	Statewide Interoperability Coordinators
TCGP	Tribal Cybersecurity Grant Program
TRIPwire	Technical Resource for Incident Prevention