Workload Staffing Model for Regional Staff

February 20, 2024

Fiscal Year 2022 Report to Congress

Homeland Security

Cybersecurity and Infrastructure Security Agency

Message from the Director

February 20, 2024

I am pleased to present the following report, "Workload Staffing Model for Regional Staff," which was prepared by the Cybersecurity Infrastructure and Security Agency (CISA).

This document was compiled pursuant to direction in House Report 117-87, which accompanies the Fiscal Year (FY) 2022 Department of Homeland Security (DHS) Appropriations Act (P.L. 117-103).

CISA provides capabilities and services to support the defense and security of the Nation's infrastructure. CISA's regional workforce is composed of Cyber Security Advisors, Protective Security Advisors, Chemical Security Inspectors, Emergency Communication Coordinators, and other support staff disbursed regionally across the United States. As CISA continues to fulfill its mission, the need to grow its regional workforce is critical for federal, state, local, and tribal stakeholders that rely on CISA's security and risk mitigation services and information. This report reflects an in-depth analysis of CISA's current structure and workload demands and summarizes CISA's plan for near-term expansion and growth.

Pursuant to congressional requirements, this report is provided to the following Members of Congress:

The Honorable David Joyce
Chairman, House Appropriations Subcommittee on Homeland Security

The Honorable Henry Cuellar
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

Inquiries relating to this report may be directed to the CISA Office of Legislative Affairs at (202) 819-2612.

Sincerely,

Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency

Executive Summary

Whether addressing cyber or physical threats or natural hazards, CISA is dedicated to working with its partners to protect critical infrastructure and enhance the Nation's resiliency. To expand its influence and support to a prioritized set of critical infrastructure owners and operators whose services are the very ones that Americans rely on every hour of every day, CISA would need to increase the number of regional personnel responsible for delivering support to the Nation's critical infrastructure owners and operators.

This report articulates the strategy and implementation plan for expanding regional capacity, to include a workload staffing model detailing the resourcing for CISA's regional staff. The conclusions put forth in this plan are predicated on national strategy documents, the national cyber threat picture, the increasing cyber-attack surface, the increased threat of domestic violent extremists, increasing impacts of natural disasters on the Nation's infrastructure, and the current and projected stakeholder needs for CISA's suite of infrastructure protection and security services and information. This plan also considers whether regional staffing requirements benefit from increasing or introducing new discipline-specific specialists to deliver new infrastructure protection and resiliency services that CISA delivers to wide acclaim to a diverse array of stakeholders via the 10 regional offices. Ultimately, this document demonstrates CISA's commitment and plan for meeting the Nation's cybersecurity and physical security goals as outlined in numerous national strategy documents (see Appendix A).

Workload Staffing Model for Regional Staff

Table of Contents

I. Legislative Language

This report was compiled in response to direction in House Report 117-87, which accompanies the Fiscal Year (FY) 2022 Department of Homeland Security Appropriations Act (P.L. 117-103).

House Report 117-87 states:

> *Security Advisors (SA).*—The recommendation includes an increase of $17,100,000 above the request to increase the number of SAs and other regional staff needed to help support CISA's regional operations. The Committee recognizes the workload in this critical area is expanding and additional resourcing is required to expand regional capacity to provide security and risk mitigation services.
>
> Not later than 90 days after the date of enactment of this Act, CISA shall report on the strategy and implementation plan for expanding regional capacity, to include a workload staffing model detailing the resourcing for Cyber Security Advisors, Physical Security Advisors, Chemical Inspectors, and other regional support staff. As part of the model, CISA shall consider whether the regional staffing requirements would benefit from introducing or increasing discipline-specific specialists.

II. Background

A. Introduction to CISA Regions

The 10 CISA regional offices enable CISA to build partnerships locally and tailor the delivery of CISA's security and risk mitigation services in the unique regional and local context of our stakeholders. Presently, 19 national strategies, executive orders, and reports outline specific goals to improve the cyber and physical security of the nation's 16 critical infrastructure sectors, with DHS designated as lead sector risk management agency for 8 sectors and the co-lead for an additional 2. Concurrently, the FY 2021 National Defense Authorization Act (NDAA) gave CISA enhanced subpoena authorities to identify and notify critical infrastructure of cybersecurity vulnerabilities. These enhanced authorities have contributed to CISA's workload. For example, in FY 2023, CISA regional personnel conducted 2,268 notifications to at-risk critical infrastructure owners and operators. For comparison, in FY 2021, the CISA regions conducted 67 notifications[1], and CISA is projected to conduct over 5,000 notifications in FY 2024. While CISA can cite year-over-year metrics to show that demand for CISA services is growing, CISA recognizes that the work to improve the resiliency and security of critical infrastructure is impossible to precisely forecast and could well be considered infinite. Therefore, CISA has developed an updated model for staffing that considers the following factors:

- Unique regional attributes such as number of states, square miles, the density of human populations and critical infrastructure;
- Emerging threats and risks to the Nation's infrastructure, such as increased cyber-attacks and the frequency and severity of natural disasters;
- The documented unfilled demand for services, such as cyber and physical vulnerability assessments and cyber incident response assistance;
- The imperative to unify CISA so that all CISA programs and services can be executed regionally in collaboration with CISA's divisions; and
- A focus on building key regional connections and relationships as the foundation of CISA's whole-of-nation approach to infrastructure security and resiliency.

Expanding the capacity and capabilities of CISA's regional offices would enable CISA to align its organizational model consistent with that of other institutions such as the Federal Bureau of Investigation (FBI)[2] or the Federal Emergency Management Agency (FEMA). More importantly, increasing CISA regional support would provide the Nation with additional highly skilled cybersecurity, physical security, chemical security, and emergency communications specialists to strengthen national and community safety, security, and resiliency. At the same time, the need for discipline-specific specialists and cyber-physical convergence specialists has grown due to the increasing complexity of the U.S. critical infrastructure ecosystem and the increasing variety of threats. In FY 2023, demand for some CISA services overwhelmed

[1] CISA Administrative Subpoena | CISA
[2] How is the FBI organized? — FBI

available capacity. This reality necessitated that CISA revisit its service portfolio and relatedly its approach to staffing. Those lessons are captured in this report.

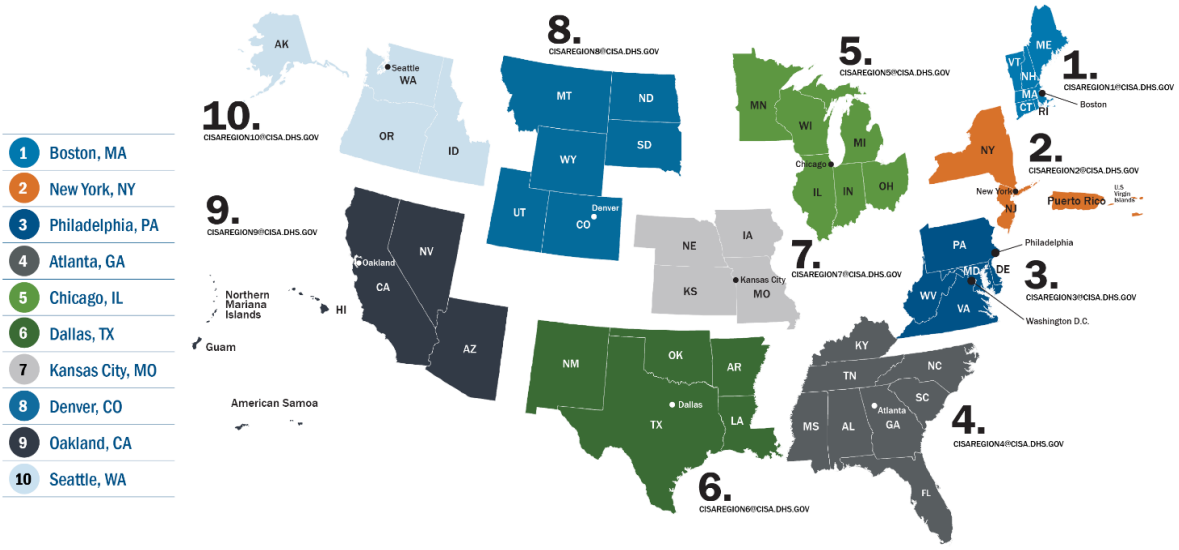

Figure 1. Map of CISA Regions and Locations of Regional Offices

B. Critical Infrastructure Risk Landscape

America's critical infrastructure underpins its advanced society and standard of living. However, this infrastructure is increasingly vulnerable to a range of cyber, physical, and natural hazard threats.

Cybersecurity

As American society becomes increasingly digitized, virtually every service imaginable is connected to and dependent upon the internet: power grids, fuel supply, transportation systems, and banking systems are just a few of these essential services. While digitization and increased connectivity has led to a more advanced society and has fostered tremendous advancements, it also presents significant risks. These risks have already manifested themselves in several ways, such as theft of intellectual property from U.S. businesses, proliferation of ransomware attacks, and attacks on the control systems that operate national critical infrastructure.

Analysis from multiple sources concludes that the emerging threats and risks posed by advanced digitization continue to rise. The rapid advance of technology in the coming decades will result in a larger cyber-attack surface. The proliferation of networked devices under the Internet of Things (IoT) coupled with 5G wireless deployment will vastly surge cyber risk and vulnerability. Other hyper-connected related technologies that will magnify cyber risks and vulnerabilities across society include: artificial intelligence and machine learning, nanotechnology, robotics, 3D printing, biotechnology, virtual/augmented reality, cloud computing, air and marine drones,

biometrics, blockchain, quantum computing and networks, distributed energy, smart grids, smart cities, autonomous vehicles, electric vehicles, web-3 technologies, non-fungible tokens, digital currencies, financial technology, the internet of space, and advanced remote sensing to name a few. Each of these technologies rely on the internet, and all will experience an increase in cyber risk.

Not only is the cyber-attack surface increasing, at the same time nation-state adversaries continue to enhance their cyber warfare institutions and capabilities. Adversaries are constantly improving their capabilities to conduct both chronic, widespread cyber campaigns, and acute, malicious cyber activity to degrade and defeat the United States.

Physical Security

Physical security threats to the Nation's infrastructure have persisted since the attacks of September 11, 2001. During the last decade these threats increased. Today, domestic violent extremists (DVE) pose a growing kinetic threat to the Nation's schools, houses of worship, electricity substations, election offices, event centers, businesses, and numerous other infrastructure facilities. The proliferation of planned and executed attacks against soft targets highlights the fact that the threat of physical violence whether state-sponsored, terroristic, or criminal in nature persists in rural, suburban, and urban communities.

Hardening such facilities and making them more secure and resilient is not a one size-fits-all-problem. Each sector and each facility within each sector require tailored security assessments and assistance. Frequently, physical security underpins cybersecurity. As a result, there is little separation today between physical and cybersecurity as the interdependence between the two increases.

Natural Hazards

Natural disasters continue to impact the Nation's critical infrastructure at an alarming rate, costing billions of dollars in damage and degrading national critical functions. These disasters often impact critical supply chains. Hurricanes, floods, and earthquakes impact an employee's ability to travel to and from their jobs in addition to halting intermodal movement of necessary goods. Intense wildfires destroy both an employee's physical workplace and torch the goods and data inside. Drought is negatively impacting access to water, including for wastewater systems and agricultural sectors. Increasing bouts of extreme heat compound the need to ensure crops and livestock have adequate amounts of water for survival. Energy and transportation sector infrastructure across the United States have experienced various natural hazard impacts. Energy grids under both extreme heat and extreme cold undergo intense strain due to increased use and potentially outdated systems and equipment. In short, the Nation's infrastructure remains fragile and vulnerable.

Natural hazards will continue to negatively impact the Nation's critical infrastructure and critical functions. Combating this threat requires that the Federal Government partner closely with state, local, tribal, territorial, and private sector entities, as well as invest in services that bolster the Nation's critical infrastructure facilities and systems.

C. The Challenge

With over 3.5 million critical infrastructure owners and operators identified in the sector specific plans of the ten DHS lead/co-lead critical infrastructure sectors[3], and an estimated 33 million small-medium business[4] across the Nation, the sheer magnitude of stakeholders in an interconnected cyber-ecosystem and supply chain is staggering.

Yet, despite the growing cyber, physical, and natural hazard risks to the Nation's infrastructure, most entities remain underprepared. The needs for improvements in security and resilience are infinite. Therefore, CISA is steadily maturing our capability to engage stakeholders and assess and understand sector risks so services and support are prioritized to return the most benefit to our nation's resilience. CISA employs rigorous governance processes to adjudicate threat information, national priorities, and regional and sector priorities so that the federal government's finite resources are applied in a way that yield the best return on investment to the Nation.

Of particular concern are organizations across the United States that lack the technical expertise to appropriately identify and mitigate risks. These organizations include many local and tribal governments, school districts, election offices, water and electric utilities, healthcare providers, scores of small and medium sized businesses, and a myriad of other critical infrastructure providers. These target rich institutions – many of whom are under resourced – provide vital services that Americans rely on every day. Helping them improve their security and resiliency is CISA's mission and a national priority.

One of the primary ways that CISA fulfills its mission as the Nation's cyber defense agency and national coordinator of infrastructure risk reduction efforts is through the delivery of services to infrastructure owners/operators, state, local, tribal, and territorial (SLTT) governments, and key private sector entities through the 10 CISA regional offices. CISA's services assist critical infrastructure owners and operators with identifying proactive steps they can take to reduce their risk exposure and increase their resiliency. Additionally, CISA is increasingly taking on the role of notifying critical infrastructure owners and operators that they have been victims of cyber-attacks or that they are in imminent danger of becoming victims of ransomware.

CISA's regional personnel also play a key role in executing CISA's information sharing responsibilities, administrative subpoena and other vulnerability notification authorities to notify critical infrastructure owners and operators that they have important systems exposed the internet. These congressionally mandated activities are best executed by regional staff leveraging their close and in-person relationships with organizations in their geographic area. However, CISA's regional personnel cover large geographical areas across several states, and their reach and impact are limited. Additionally, as local officials and critical infrastructure owner and operators get more familiar with CISA, regional personnel are highly sought after to participate in advisory forums with local leaders, security conferences, give presentations and keynotes. CISA estimates that regional offices defer 20 percent of requests for services such as

[3] Sector Risk Management Agencies | CISA
[4] Frequently Asked Questions About Small Business 2023 – SBA's Office of Advocacy

exercises, training, workshops, and analytic support by 6 months or more due to the high day-to-day workload.

D. The Opportunity

To more effectively engage and partner with the Nation's critical infrastructure owners, operators, and businesses, and to prepare and support them in addressing national and economic security needs and the health/safety challenges posed by the increased threats to the Nation's infrastructure, there is a need to expand CISA's regional workforce.

III. Regional Model Benefits

A. Advantages

The United States has thousands of infrastructure facilities and systems that span the entirety of the 50 states and U.S. territories. Increasing national infrastructure resilience requires active engagement with infrastructure owners and operators where they live and work. Deploying security advisors in all 50 states, territories, and the District of Columbia offers the advantages described below.

Builds Relationships

CISA's regional security advisors live in the communities where they work. Through direct in-person engagements with SLTT officials, infrastructure operators, and industry stakeholders, regional staff forge relationships and establish credibility. Stakeholders are more receptive to sharing information and partnering with CISA as a result of the trust engendered. Achieving cyber and physical resiliency will take a whole-of-nation effort underpinned by the trust and relationships that comes from CISA's regional presence.

Provides Context

Managing risk requires context and understanding of the operational environment. CISA regional staff develop deep knowledge of the industries, institutions, and infrastructure in their region and are able to assess the local, regional, and national impact of incidents and adverse events in their region. They also understand the regional variations in law, governance, and philosophy and can adapt national response to make sense locally. By tailoring CISA programs and services to the characteristics of each region, field staff are able to foster trust and optimize risk mitigation.

Increases Agility

Each region maintains a regional headquarters office in a key city that is home to other federal partner offices and state and local fusion centers. Beyond the regional headquarters office, CISA staff, namely security advisors, are hired in close geographical proximity to key critical infrastructure locations across the regions. Hiring staff in close proximity to the infrastructure they serve cuts down on their travel time and reduces costs. By pre-positioning regional staff near constituents, CISA can rapidly deploy and deliver in-person cybersecurity, physical security, chemical security, and emergency communications assistance to stakeholders within hours anywhere in the nation by eliminating long haul travel delays and logistics associated with air or train travel.

In sum, the CISA regional service delivery model, which builds on best practices from years of building relationships and advising critical infrastructure stakeholders, provides numerous operational and fiscal advantages. The following sections outline a plan to expand CISA

regional offices to better implement CISA's programs and priorities and achieve even greater results in improving the security and resiliency of the Nation's critical infrastructure.

B. Services and Support

CISA regional offices deliver a wide range of services and support designed to improve various aspects of the security and resiliency of critical infrastructure assets, facilities, and systems. These services and support options are organized around five regional lines of effort:

Vulnerability Assessments

Vulnerability assessments form the core of CISA's regionally delivered physical and cybersecurity services. The first step in reducing risk is to identify risk. CISA's suite of free and voluntary physical and cybersecurity assessments are designed specifically to aid SLTT governments, critical infrastructure operators in all 16 sectors, and key businesses in identifying their vulnerabilities to cyber intrusions, physical attacks, and natural hazards acting to reduce risk.

Cyber and Physical Stakeholder Preparedness

Improving both the physical and cyber security and resiliency of critical infrastructure facilities, SLTT governments, and industry is best achieved when CISA engages stakeholders in preparedness activities before an incident or a disaster occurs. These preparedness activities come in a variety of forms including: the delivery of training and education courses, designing and conducting exercises, planning technical assistance, and conducting workshops on all cyber and physical resiliency topics. Each of these services provided by the CISA regions build the capabilities and capacity of stakeholders to reduce risk and improve security.

Threat and Risk Information Sharing

CISA regions raise awareness and understanding of cyber and physical threats through a host of unclassified and classified information sharing systems. Threat and risk information educates and informs critical infrastructure operators, SLTT officials, business leaders, and others on emerging threats, risks, vulnerabilities, and mitigation measures with the aim of protecting vital infrastructure systems and services. Open and collaborative information sharing with CISA's many partners is a core tenet and service of the CISA regions.

Special Event and Incident Response Operations

CISA regions provide planning and security operations assistance for community special events. They also provide risk advice to state and local officials leading up to and during National Security Special Events and incidents and disasters as part of CISA's responsibilities under the National Response Framework, National Disaster Recovery Framework, and National Cyber Incident Response Plan.

Partnership Development, Risk Advice, and Assistance

Effective relationships are the key to success. CISA regional staff convene and participate in cross-discipline and interagency working groups and taskforces to identify problems and develop joint solutions to all types of physical, cyber, and natural hazard threats to the Nation's infrastructure.

C. Roles

Regional staff and security advisors located in all 50 states and some U.S. territories deliver the services outlined above. Security advisors, sometimes thought of as risk advisors, are in close physical proximity to CISA's customers in order to best serve them. Security advisors are supported by outreach and analytics teams and operational support staff located in each of CISA's 10 regional office headquarters.

Security Advisors are organized in the following roles described below:

1. Cyber Security Advisors (CSA)
2. Cybersecurity State Coordinators (CSC)
3. Protective Security Advisors (PSA)
4. Chemical Security Inspectors (CSI)
5. Emergency Communications Coordinators (ECC)
6. Election Security Advisors (ESA)
7. Operational Support and Analytics

Cyber Security Advisors

CSAs share cyber threat information, conduct cybersecurity vulnerability assessments, and provide other services to assist organizations with protecting their networks and enhancing their cybersecurity programs. They are enabled by cybersecurity analysts and other CISA regional office cybersecurity professionals to provide cyber technical 'assistance and services directly to infrastructure facility operators, SLTT government agencies, and key industries. CSA responsibilities include:

- Conducting Cyber Protection Visits (CPV) with SLTT governments and infrastructure facility information technology and cybersecurity staff to understand their cybersecurity gaps/challenges and offer targeted cybersecurity services based on client needs.
- Delivering Targeted Notifications to entities of potential cyber vulnerabilities on their networks. These 'duty to warn' notifications made to public and private sector entities help mitigate problems before they occur.
- Providing assessment services that include, but are not limited to, Cyber Performance Goal Assessments, Cyber Resilience Reviews, External Dependencies Management, Cyber Infrastructure Surveys, and others as developed and deployed.
- Conducting a variety of Cyber Education and Awareness presentations and briefings to a wide array of technical and non-technical audiences to educate stakeholders on the cyber

adversarial threat, cyber vulnerabilities, and best practices in mitigation measures/controls. Priorities include state and local election officials, water and wastewater operators, K-12 school districts, healthcare institutions, and many others.
- Providing Cybersecurity Working Group Leadership for numerous federal and state interagency cybersecurity taskforces and working groups bringing together government and private sector IT security officials to share cyber threat information and develop joint cyber defense solutions.

FY 2022 CSA activities:

- Delivered over 900 cybersecurity vulnerability assessments across the United States to critical infrastructure facilities, SLTT governments, and key industries. The purpose of these voluntary assessments is to improve the cybersecurity risk management policies and procedures of the client.
- Conducted over 1,000 CPVs to understand stakeholder cybersecurity challenges and assess their needs.
- Performed over 100 targeted notifications to infrastructure facilities to warn them of potential cyber vulnerabilities.
- Conducted hundreds of cybersecurity awareness briefings at conferences and workshops.
- Led or participated in hundreds of cybersecurity working groups and task forces across the United States.

Cybersecurity services are in the highest demand from CISA's stakeholders. Threats to critical infrastructure from cyber-enabled means is one of the Nation's top national security threats. The deployment of CISA regional CSAs and cyber analysts to every state in the Nation is critical for enabling CISA to provide cybersecurity services CISA's stakeholders need. The outcome is a more secure cyber ecosystem across the country.

Cybersecurity State Coordinators

CSCs are CSAs who have been hired to work with a specific state to fulfill requirements outlined within the FY 2021 NDAA. In many instances, additional CISA personnel within the regional offices possess the required cybersecurity qualifications, expertise, and capabilities to support these requirements. For example, a CSA can support these requirements. These individuals have the same skillsets, have similar duties, and can augment the work of CSCs. In case of a vacancy, a CSA can perform most of the CSC functions listed below. CSCs hold non-supervisory positions and report directly to their respective region's Chief of Cybersecurity or Supervisory CSAs.

The statutory duties of the CSC as defined in the NDAA include:
- Build strategic partnerships with public, and private sector entities, including advising on establishing governance structures to facilitate the development and maintenance of secure and resilient infrastructure within their dedicated area of responsibility.

- Augment entities within their specified state as a federal cybersecurity risk advisor supporting preparation, response, and remediation efforts on cybersecurity risks and incidents.
- Facilitate the sharing of cyber threat information to improve understanding of cybersecurity risks and situational awareness of the current cyber landscape.
- Coordinate the sharing of applicable financial, technical, and operational resources available from the federal government to increase resilience against cyber threats.
- Augment entities within each CSC's respective state by supporting training, exercises, and planning for continuity of operations to expedite recovery from cybersecurity incidents and other disruptive events.
- Upon request from the CSC's respective state, serve as a principal point of contact for non-federal entities to engage with the federal government on preparing, managing, and responding to cybersecurity incidents.
- Help non-federal entities to develop and coordinate vulnerability disclosure programs consistent with federal and information security industry standards.
- Upon request from SLTT governments, assist in developing state cybersecurity plans.

Protective Security Advisors

PSAs are trained subject matter experts in physical security, critical infrastructure protection and resiliency, and vulnerability mitigation. PSAs provide facility and systems level assessments, training deliveries, exercise support, special event security assistance, incident response support and other services to improve the security and resiliency of infrastructure facilities and government offices. PSA responsibilities include:

- Delivering free and voluntary physical security vulnerability assessments to critical infrastructure operators, SLTT governments and select private enterprises to improve their physical security posture. In response to world events, PSAs have adapted to provide services to nonprofit organizations, K-12 educational facilities, and state and local election offices.
- Performing sophisticated multiyear critical infrastructure systems level studies that cover entire regions or states. These studies known as Regional Resilience Assessment Programs (RRAP) analyze security or resiliency challenges across entire states or sectors and provide resiliency enhancement options to stakeholders to improve infrastructure security and resiliency at a systems level.
- Providing trainings, seminars, and presentations to assist public and private sector stakeholders better secure their facilities and staff. This myriad of trainings is provided to all sectors and includes things such as K-12 school security, active shooter preparedness, securing public gatherings, and headquarters-developed trainings like Bomb-Making Awareness Courses, etc.
- Contributing to the planning and security of special events. These include National Special Security Events and Special Event Activity Rating Events throughout the United States.

- Leading CISA's incident response efforts as part of CISA's responsibilities under the National Response Framework and National Disaster Recovery Framework. PSAs routinely deploy to federal, state, or local Emergency Operations Centers to advise emergency response officials on response and restoration priorities regarding critical infrastructure assets and systems.
- Convening and participating in numerous security working groups from State Election Security Working Groups to Hate Crimes Taskforces to Electricity Substation Task Groups among many others. Whether the topic is port security, commercial facilities security, school security, or fuels systems resiliency, PSAs are trusted partners that are always available to advise on risk management approaches.

FY 2022 PSA activities:

- Delivered over 900 physical security assessments of key state and local government offices and critical infrastructure facilities.
- Conducted hundreds of data analysis meetings with partners to complete 13 systems level RRAP studies.
- Conducted thousands of physical security trainings for a wide array of stakeholder groups.
- Helped to plan for or participated in security operations for over 100 special events.
- Served in 10 federal disaster operations and assisted state and local authorities in hundreds of lesser incidents across the country.
- Led or served on hundreds of Working Groups and Taskforces throughout the United States related to improving the security of infrastructure sectors.

Since CY 2004, PSAs have provided security expertise to all critical infrastructure sectors. As the security threat and technologies changed, PSAs adapted to provide state-of-the-art security advice and assistance to all varieties of stakeholders. PSAs enable advanced security protections around the United States from schools and houses of worship to substations and clinics.

Chemical Security Inspectors

CSIs advise and assist facilities containing hazardous chemicals on security measures to reduce the risk of its chemicals being weaponized. For facilities covered under the Chemical Facility Anti-Terrorism Standards (CFATS) program per 6 C.F.R Part 27, this includes working with the highest risk chemical facilities to develop security plans and conduct inspections to ensure that security is in place. CSI responsibilities include:

- Performing inspections and enforce compliance with CFATS standards through Authorization Inspections, Compliance Inspections, and Compliance Assistance Visits and support and respond to incidents at chemical facilities.
- Assisting regulated chemical facilities writing security plans to ensure optimal security measures are in place. CSIs also meet with a wide variety of industry representatives and conduct workshops on best practices in securing precursor bomb-making chemicals.

- In collaboration with FBI field offices, meeting with major retailers to raise awareness to help recognize and report suspicious activity regarding the purchase of precursor bomb-making materials.
- Operating the "Chemlock" Voluntary Chemical Security Program. While regulatory programs cover tiered facilities that possess high quantities of precursor bomb-making material, regulated entities represent a tiny fraction of the tens-of-thousands of facilities that possess dangerous chemicals but fall below regulation thresholds. The theft, diversion, or purchase of these chemicals by nefarious actors can be used to fashion improvised explosive devices (IED).

FY 2022 CSI activities:

- Conducted 140 Authorization Inspections and 1,681 Compliance Inspections of regulated facilities.
- Conducted hundreds of security planning meetings and other outreach activities with industry.
- Conducted over 2,300 engagements with retail locations under Operation Flashpoint.
- Provided onsite technical security assistance and training on a voluntary basis to thousands of non-CFATS facilities around the country that possess large volumes of IED precursor chemicals under the "Chemlock" Program.

Every day, thousands of chemical facilities across the United States – from small companies to large industrial plants – use, manufacture, store, and transport hazardous chemicals in a complex supply-chain impacting virtually all other infrastructure sectors. CSIs reduce the risk that these hazardous chemicals pose to the Nation.

Emergency Communications Coordinators

ECCs enhance emergency communications interoperability by providing training, tools, workshops, and planning assistance to local, state, and private sector public safety communications officials. These services assist stakeholders by ensuring they have communications during steady-state and emergency operations. Through these services, ECCs work to ensure first responders and public safety officials can seamlessly and securely communicate. Their responsibilities include:

- Delivering services related to emergency communications preparation and planning by supporting the development and maintenance of statewide government structures and working closely with executive leaders in government to sustain statewide interoperability executive councils. The ECCs serve as telecommunications subject matter experts to improve nationwide network resiliency planning and operational capabilities.
- Working directly with states to identify user needs and coordinate the delivery of direct technical assistance via the congressionally mandated Interoperable Communications Technical Assistance Program. Examples of services include 911 call center vulnerability assessments and communications technician and dispatcher courses.
- Providing communications planning and direct support to large-scale special events to ensure security officials at all levels can maintain interoperable communications.

- Aiding in restoring both public and private sector telecommunications following federally declared disasters in support of states and FEMA under the National Response Framework.

FY 2022 ECC activities:

- Contributed to the publication of 15 Statewide and Tactical Communications Interoperability Plans.
- Delivered 199 technical assistance offerings to state and local officials.
- Supported numerous special events around the country.
- Deployed to five natural disasters in the United States and assisted the Department of State in the Dominican Republic to help restore telecommunications.

CISA's cadre of ECCs across the country assist local community and state level public safety organizations. ECCs enable CISA to improve operational technical assistance and risk management advice to both public and private sector telecommunications entities to improve emergency communications reliability for the United States.

Elections Security Advisors

CISA is currently in the process of hiring ESAs, which will be assigned to each of the CISA regions. This position will report directly to the Regional Director and will lead regional elections security engagement strategies (in partnership with current field staff) to support state and local election officials throughout the United States helping to enhance both the cybersecurity and physical security of elections systems, processes, and facilities. ESAs will:

- Lead the region's election security engagement strategy to support state and local election officials.
- Recommend new products, training, assistance, and services based on detailed knowledge of election infrastructure stakeholder requirements and knowledge of emerging approaches to assess and mitigate cyber, physical and operational risks.
- Communicate the value of election security throughout all levels of internal and external stakeholders.
- Participate in partnerships with election infrastructure partners. Promote collaborative efforts to reduce risks and threats to critical information, enterprise, communications, and control systems.
- Raise awareness and improve coordination with state and local governments on CISA's support to election infrastructure.
- Participate in the establishment of community-based, regional, and/or statewide election security strategies for election infrastructure stakeholders.
- Evaluate election infrastructure stakeholders needs to identify specific opportunities where CISA provide support, resources, and services for election infrastructure stakeholders.

The safety, security, and resiliency of elections remains one of the agency's top priorities. The establishment of the ESA position in each of CISA's regional offices is an acknowledgement and

further recognition of the criticality our elections security mission and is in alignment with our priority to field additional resources, experience and expertise to the field in order to better support our stakeholders throughout the nation.

Operational Support and Analytics

Regional operations and analytics staff enable CISA's cybersecurity and physical security services to scale to more critical infrastructure owners and operators by delivery of training courses and exercises, workshops, data analytics and fusion, information sharing, incident management support, and external affairs services. Staff assist Security Advisors by arming them with information and analytics that will help tailor engagements to each unique customer's needs. Operations and analytics staff responsibilities include:

- ***Exercises*** – CISA regions organize, plan, and deliver cybersecurity and physical security exercises for stakeholders. These exercises test facility plans and procedures, identify gaps, and document best practices. CISA provides stakeholders with an After-Action Report that offers tangible steps to improve their cyber and/or physical security posture. Cyber incident response tabletop exercises are in especially high demand by a myriad of stakeholders including state and local election officials, water utility associations, K-12 school districts, healthcare facilities, and many others.
- ***Trainings*** – Regional personnel coordinate the delivery of training courses to critical infrastructure owners and operators. One of the most requested training courses is Active Shooter Preparedness training. Additionally, regions connect stakeholders with CISA's Office of Bombing Prevention courses such as IED Awareness training. Regions also organize sector specific trainings offered by the Sector Risk Management Agencies (SRMA) on topics such as critical manufacturing supply-risk management and dams security.
- ***Workshops*** – CISA regions deliver a suite of workshops to introduce physical and cyber resilience concepts to stakeholders to improve their security programs/postures. Workshop topics include cybersecurity, insider threat, election security, cybersecurity education, security symposiums, and school safety.
- ***Data Analytics*** – Regions determine impacts to critical infrastructure and cross-sector impacts in preparation for and in response to an incident. Regional staff also determine dependencies and cascading effects on critical infrastructure and potential impacts to supply chains. CISA regions provide geospatial products and infrastructure planning support to assist Security Advisors, FEMA crisis action teams, state emergency management and fusion centers, and other partners.
- ***Analytical Support and Information Sharing*** – Regional personnel compile, synthesize, and share cyber and physical security threat information such as alerts, warnings, directives, bulletins, analysis reports, and advisories with a wide-range of critical infrastructure sector stakeholders.
- ***External Affairs*** – CISA regions engage professional associations and social and traditional media to communicate to raise awareness and increase understanding of cyber and physical security actions to keep institutions and the American people safe.
- ***State, Local, Tribal and Private Sector Clearance Program*** – Regions nominate and maintain a cadre of cleared partners to include State Election Officials, State Chief

Information Security Officers, Utility Security Officers, and others. Partners with a security clearance participate in classified briefings and receive classified information on a need-to-know basis. This information enables stakeholders to get ahead of potential problems.

FY 2022 Operational Support and Analytics Activities:

- Conducted approximately 200 exercises for critical infrastructure owners and operators.
- Delivered several hundred virtual and in-person trainings for stakeholders.
- Delivered thousands of threat alerts and other informational products to stakeholders to assist security decision-making.
- Delivered scores of workshops for stakeholders on a range of cybersecurity, emergency communications, and physical security topics.
- Produced analytical products to assist stakeholders in making informed risk mitigation decisions.
- Provided articles and interviews with print, television, radio, social media, and professional groups' newsletters on physical and cybersecurity best practices and actions.
- Organized classified briefings for these cleared officials to enable action.

Cybersecurity and physical security preparedness services are the key to improving the resiliency posture of organizations before a crisis hits. CISA's cyber and physical preparedness service deliveries such as training courses, exercises, and analytical products help CISA's stakeholders significantly improve the resiliency of the Nation's infrastructure.

D. Regional Size and Staff Composition

To determine the appropriate size and composition of its regional offices, CISA considered several quantitative and qualitative inputs.

Key Factors Considered

- **Regional Attributes:** Each regional office has unique attributes such as the number of states and territories it serves, geographic size, population density, the number of major urban centers and tribal nations, the number of FBI field offices and state fusion centers, the density and concentration of infrastructure sectors and facilities, etc. Each CISA region staffing plan must be 'right sized' to match the characteristics of the constituency it serves.
- **Emerging Threats and Risks:** Several predictions of the future threat landscape are treated as facts in the staffing analysis: (1) the increasing cyber-attack surface; (2) the deployment of new technologies such as artificial intelligence and 5G increases the complexity of infrastructure protection; and (3) the increase in cyber and physical threats to infrastructure from nation-states, natural hazards, and violent extremists.
- **National Security Strategies and Directives:** From cybersecurity to countering violent extremism and climate change adaptation, numerous White House, DHS, congressional and other national strategies and reports direct CISA to support. CISA's regional force

structure outlined in this plan incorporates the staff necessary to pursue and achieve the goals outlined in these national strategies.

- **Number of Stakeholders:** Infrastructure operators, K-12 school districts, public utilities, local governments, and all varieties of stakeholder's clamor for CISA's infrastructure security services. Having sufficient staff in place to meet stakeholder requests for services is an important variable in the regional office staffing model.
- **Key Regional Connections:** Infrastructure protection requires cooperation. Success will hinge on relationships and joint problem solving with other federal agencies, technology companies, state institutions, professional associations, and so forth. Additional staff are needed to liaise with and advise state, federal, and industry working groups and associations.

Service and Support Vision

With over 33 million small business and millions of critical infrastructure sector constituents composing the ecosystem that delivers the services and functions the Nation relies on, CISA must proactively engage to improve national resilience and stand prepared to rapidly respond to, contain, mitigate and recover from adverse events.

Due to the overwhelming number of potential stakeholders and near-infinite demands for support, it would not be practical to resource CISA to directly meet stakeholder demand. More realistically, CISA seeks to position itself to rapidly respond to national security threats and significant incidents, and to proactively partner and engage with critical infrastructure owners and operators at sufficient frequency and volume to influence and effect changes that mature National resilience and reduce risk.

CISA envisions a future where the agency is positioned to rapidly support incident management across the nation. This vision requires that every state and territory has an assigned team to handle incident management, where at least one cybersecurity advisor is based in every metropolitan area with a population of 100,000 or more, and where CISA coordinates even more closely and frequently with state, local, tribal and territorial governments, other federal partners, and critical infrastructure owners and operators to collectively manage risks to the Nation.

Meeting the Need

Cybersecurity Advisors

To be effective, CISA must build and maintain trust and credibility, and provide timely support. With at least 2.4 million critical infrastructure owners and operators under the 8 critical infrastructure sectors CISA is responsible for, and the estimated 33 million small-medium businesses, there is simply no practical demand-based staffing model. Even if we assumed a demand rate as low as 10 percent this would mean over 240,000 critical infrastructure

stakeholder engagements. To meet this theoretical demand, based on an average of 9.1 hours per engagement[5], it would require 1,625 Cybersecurity Advisors.

In light of overwhelming resources needed to meet even the most conservative demand estimate, CISA instead believes a more practical model that balances cost, demand and mission need with a reasonable number of resources is best positioned to support the most stakeholders and engage in risk planning and response efforts with local context and understanding.

CISA estimates 698 Cybersecurity Advisors geographically assigned to major urban centers with a population of 300,000 or greater are needed. To minimize travel overhead, increase agility, and maximize engagements and exposure, CISA's workforce model has a long-term goal to assign one CSA to every Metropolitan Statistical Area (MSA) with a population greater than or equal to 100,000; however, the current model maintains more feasible near-term hiring targets and assumes one CSA per MSA with 300,000 people. These CSAs will focus on building trust and credibility with the critical infrastructure operators in their region, ultimately enabling CISA influence sector actions while supporting individual stakeholders.

The CSAs will in turn work in close coordination with their regional cyber chiefs (1 per region) and cybersecurity state coordinators (1 per state). Regional cyber chiefs and state coordinators will be primarily responsible for coordinating with SLTT government counterparts and other federal partners to contextualize threats, and risks, develop operational strategies, and prioritize engagements in such a way to minimize regional and local risks and maximize return on this investment of resources.

To provide for deep technical expertise well versed in local laws, statutes, policies and politics capable of supporting effective response and recovery efforts in incidents that disrupt and degrade delivery of critical services and functions, CISA's workforce model also assigns one Cyber Defense Team comprised of five multi-disciplinary[6] CSAs to each state, equally ready for instant deployment or proactive engagement.

Finally, while no two support engagements are ever truly identical, the average CSA engagements takes 9.1 hours to complete and CISA estimates that each Cyber Defense Team engagement will take 130 hours to complete. CISA's workload model would support up to 50 thousand critical infrastructure operators and up to 517 significant response and recovery efforts across the nation.

Protective Security Advisors

SLTT and critical infrastructure organizations, especially under resourced small and medium businesses, have little choice but to rely on federal support and assistance to report and respond to incidents, understand dynamically changing threats and manage risk. The adoption and integration of IoT and Industrial IoT devices have led to an increasingly interconnected mesh of cyber-physical systems, which expands the attack surface and blurs the once clear functions of

[5] On average advisors spend 9.1 hours per engagement including 2.5 hours or logistics and preparation, 1.7 hours in travel, 3.45 hour of engagement, and an additional 1.45 hours in post engagement follow-up.
[6] (1) Team Lead, (2) IT Specialist, (3) OT Specialist, (4) Networking Specialist, (5) Cloud/Data Specialist

cybersecurity and physical security. CISA must take steps to enhance the technical skills, depth, and availability of regional resources to meet and address cyber/physical convergence and the national demand for support and assistance. Positions focused on cyber/physical convergence builds CISA's field expertise and capability. CISA's field forces will then work directly with SLTT and private sector partners to understand local and regional risk across sectors. Additional resources in the field will result in CISA gaining a better understanding of the compounding impacts of cyber and physical convergence.

PSAs serve the same stakeholders and have the same stakeholder demand as Cyber Security Advisors. Here again, to meet even the most modest demand-based service model would require engaging with hundreds of thousands of stakeholders annually. CISA again proposes a more practical model that utilizes a reasonable number of resources positioned to advise and support the most stakeholders by increasing staff to ensure there is one PSA per MSA with populations greater than 300,000 as well as Urban Area Security Initiative (UASI) cities.

Emergency Communications Coordinators

Emergency Communications staffing lags behind the PSA, CSA, and CSI cadres and are a critical pillar of the overall expertise and capability CISA provides to its stakeholders. Public Safety Answering Points, 911 call centers, and emergency communications nodes remain attractive targets for adversaries and increased capacity will improve incident coordination, information sharing, and increase relationships and partnerships with the emergency communications sector and its myriad of stakeholders.

Achieving one ECC per state and the territories of Puerto Rico and Guam would enable the CISA regions to have sufficient staff to collaborate, synchronize and coordinate products, services, and feedback across the various CISA divisions and security disciplines.

Operational Support and Analysis

As the regional security advisor footprint increases to meet the needs of the nation, our regional operations and analytics staff must scale to meet the increased demand of service delivery to include training courses and exercises, workshops, data analytics and fusion, information sharing, and incident management support to critical infrastructure owners and operators. These individuals are key to ensure the security advisors are prepared and well-informed to provide tailored and impactful engagements. The number of CISA's operational support and analysis staff must grow proportionally with the security advisors. CISA estimates that for every 15 security advisors the number of operational and analytic support staff must increase by one to keep pace with the growing operational and analytical needs.

Workforce Staffing Summary

Consistent with the workload model, the following table summarizes CISA's short-term workforce staffing needs:

Table 1. CISA Regional Workforce Staffing Needs

Role	Authorized Staffing	Target Staffing	Additional Needed	Assumptions
Cyber Security Advisors	166	328	+162	• Additional CSA to support the growth toward 1 CSA in every MSA with a population >= 300,000 • 1 five-person Cyber Defense Team per Region
Protective Security Advisors	184	250	+66	• Additional Protective Security Advisors to support the growth toward 1 PSA in every MSA with a population >= 300,000 • 1 PSA per UASI city
Election Security Advisors	10	10	0	• No change
Emergency Communication Coordinators	20	55	+35	• 1 ECC per State and the Territories of Guam and Puerto Rico
Operational Support and Analysis	118	118	0	• No change
Chemical Security Inspectors	182	182	0	• No change
Leadership	20	20	0	• No Change
Totals	**700**	**963**	**+263**	

Resources in Action

In addition to being the lead/co-lead SRMA for 8 critical infrastructure sectors representing over 2.6 million stakeholders, for FY 2024 CISA has identified the People's Republic of China (PRC) as a top threat to address across all sectors and securing elections as a top priority.

If the growth in Table 1 is realized, IOD would be able to support up to 30,000 engagements including:

- 3,000 engagements in each of CISA's SRMA sectors;
- 4,000 election engagements including at least one with every county across the United States and each state secretary of state;

- 2,000 resilience efforts directed towards organizations at increased risk from the PRC; and
- 10 advanced incident response and recovery advisory efforts per region.

IV. Conclusion

By investing in CISA's regional offices and security advisor cadre located in every state, CISA can begin to scale its physical and cybersecurity services to meaningfully bend the national risk curve downward. Without significant advancements to the cyber defenses and physical security of critical infrastructure, the peril to national security, national economic security, and public health/safety will only increase. This report supports CISA's strategy throughout the Planning, Programming, Budget, and Execution process to enable CISA to bolster its services across the Nation to reduce the growing risk to the Nation's infrastructure, governments, and key industries. The additional resources derived from this model would improve cyber resilience and preserve and protect the Nation's critical infrastructure, and national security.

V. Appendices

Appendix A: National Security Directives

The White House, *National Cybersecurity Strategy*, 2023

The White House, *National Security Strategy*, 2022

The White House, *National Strategy for Control Systems Security*, 2020

The White House, *National Cyber Strategy of the United States of America*, 2018

The White House, *National Cyber Moonshot*, 2018

The White House, *PPD-21, Critical Infrastructure Security and Resilience*, 2013

The White House, *PPD-41, United States Cyber Incident Coordination*, 2016

The White House, *Executive Order on Improving the Nation's Cybersecurity*, 2021

The White House, *Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries*, 2021

Cyberspace Solarium Commission, *Cyberspace Solarium Commission Report*, 2020

U.S. Department of Homeland Security, *DHS Strategic Plan FY2022-2026*, 2023

U.S Department of Homeland Security, *Secretary Mayorkas, Department wide 2022 priorities memorandum*, March 13, 2022

U.S. Department of Homeland Security, *DHS Cybersecurity Strategy*, May 15, 2018

U.S. Department of Homeland Security*, Strategic Framework for Countering Terrorism and Targeted Violence*, 2019

U.S. Department of Homeland Security, *National Cyber Incident Response Plan*, 2016

U.S. Department of Homeland Security, *National Response Framework*, 2019

U.S. Department of Homeland Security, *National Disaster Recovery Framework*, 2016

U.S. Department of Defense, *National Defense Strategy of the United States*, 2022

CISA, *CISA Strategic Plan 2023-2025*, 2022

CISA, *A System at Risk – Partnering to Safeguard K-12 Education Entities from Cyber Threats*, December 2022.

Multi-State Information Sharing and Analysis Center, *Nationwide Cybersecurity Review, Summary Report*, 2021

Appendix B: Abbreviations

Abbreviations	Definitions
CFATS	Chemical Facility Anti-Terrorism Standards
CSA	Cybersecurity Advisor
CSI	Chemical Security Inspector
CPV	Cyber Protection Visit
CY	Calendar Year
ECC	Emergency Communications Coordinator
FY	Fiscal Year
IED	Improvised Explosive Device
IoT	Internet of Things
NSSE	National Special Security Event
PRC	People's Republic of China
PSA	Protective Security Advisor
RRAP	Regional Resilience Assessment Program
SLTT	State, Local, Tribal, and Territorial
SRMA	Sector Risk Management Agency
UASI	Urban Area Security Initiative