

Cybersecurity & Infrastructure Security Agency (CISA) Information, Resources & Quick Links – May 21, 2024

The Department of Homeland Security’s (DHS) Cybersecurity & Infrastructure Security Agency (CISA) is one of many federal agencies with completely voluntary cybersecurity resources and offerings for the sixteen critical infrastructure sectors – including the healthcare industry. Also, check out our “[Free Federal Government Cybersecurity Resources](#)” Cheat Sheet for additional cyber resources offered by other federal agencies.

The Top 3, no-cost cybersecurity services CISA offers are:

- 1) [Connect with your Regional Cybersecurity Advisor \(CSA\)](#) – CISA's program of work is carried out across the nation by personnel assigned to its 10 regional offices. Regions are based on your state. See below for a handy chart of CISA Regional Offices & Contact Information.
- 2) [Sign up for Cyber Hygiene Services](#) – CISA's Cyber Hygiene services help secure internet-facing systems from weak configurations and known vulnerabilities.
- 3) [Cybersecurity Performance Goal \(CPG\) Assessment](#) – CISA's CPGs are a common set of practices all organizations should implement to kickstart their cybersecurity efforts. Small and medium-sized organizations can use the CPGs to prioritize investment in a limited number of essential actions with high-impact security outcomes. CISA has mapped the free services in their Free Cybersecurity Tool & Services [database](#) to the CPGs to aid prioritization of risk-reduction efforts.

Additionally, CISA offers:

- No-cost, in-house cybersecurity services designed to help individuals and organizations build and maintain a robust and resilient cyber framework.
- An extensive selection of free cybersecurity services and tools provided by the private and public sector to help organizations further advance their security capabilities.

Free Cybersecurity Services and Tools

CISA has curated a database of free cybersecurity services and tools as part of their continuing mission to reduce cybersecurity risk across U.S. critical infrastructure partners and state, local, tribal, and territorial (SLTT) governments. In addition to offering a range of no-cost CISA-provided cybersecurity services, CISA has compiled a list of free services and tools provided by private and public sector organizations across the cyber community. You can find more information [here](#). For additional information or questions related to CISA-Provided cybersecurity services, email Central@cisa.gov.

Additionally, you can browse the following cybersecurity services and tools:

- [CISA-Provided Cybersecurity Services](#) – A single database that provides users with access to information on CISA cybersecurity services that are available to our stakeholders free of charge.
- [Free Non-CISA Cybersecurity Services](#) – Browse a list of free cybersecurity services and tools, which are provided by private and public sector organizations across the cyber community.
- [Cybersecurity Resources for High-Risk Communities](#) – Discover the suite of tools and services that CISA, industry, and civil society partners offer to high-risk communities.

Reporting a Cyber Incident

CISA provides secure means for constituents and partners to report incidents, phishing attempts, malware, and vulnerabilities. You can submit reports [here](#). Organizations can also report anomalous cyber activity and/or cyber incidents by emailing report@cisa.gov, or calling [1-844-Say-CISA](tel:1-844-Say-CISA) (1-844-729-2472).

The [Federal Bureau of Investigation \(FBI\)](#) is the lead federal agency for investigating cyberattacks and intrusions. They collect and share intelligence and engage with victims while working to unmask those committing malicious cyber activities, wherever they are. If you or your organization is the victim of a network intrusion, data breach, or ransomware attack, contact your [nearest FBI field office](#) or report it at tips.fbi.gov.

Additional CISA Cyber Resources & Quick Links

[Secure Our World](#) – Simple ways to protect yourself, your family and your business from online threats.

[Shields Up](#) – As the nation’s cyber defense agency, CISA stands ready to help organizations prepare for, respond to, and mitigate the impact of cyberattacks.

[Stop Ransomware](#) – Ransomware Guidance and Resources

CISA Regional Offices & Contact Information

REGION	HQ	STATES/TERRITORIES	CONTACT
1	Boston, MA	CT, MA, ME, NH, RI, VT	CISARegion1@hq.dhs.gov
2	New York, NY	NJ, NY, PR & US VI	CISARegion2@hq.dhs.gov
3	Philadelphia, PA & Washington, DC	DE, DC, MD, PA, VA, WV	CISARegion3@hq.dhs.gov
4	Atlanta, GA	AL, FL, GA, KY, MS, NC, SC, TN	CISARegion4@hq.dhs.gov
5	Chicago, IL	IL, IN, MI, MN, OH, WI	CISARegion5@hq.dhs.gov
6	Dallas, TX	AR, LA, NM, OK, TX	CISARegion6@hq.dhs.gov
7	Kansas City, MO	IA, KS, MO, NE	CISARegion7@hq.dhs.gov
8	Denver, CO	CO, MT, ND, SD, UT, WY	CISARegion8@hq.dhs.gov
9	Menlo Park, CA	AZ, CA, HI, NV, American Samoa, Guam, and the Pacific Islands	CISARegion9@hq.dhs.gov
10	Seattle, WA	AK, ID, OR, WA	CISARegion10@hq.dhs.gov

Within each CISA Region are your local and regional Protective Security Advisors (PSAs), Cyber Security Advisors (CSAs), Emergency Communications Coordinators (ECCs), Election Security Advisors (ESAs) and Chemical Security Inspectors (CSIs). In order to build stakeholder resiliency and form partnerships, these field personnel assess, advise, and assist and provide a variety of risk management and response services.