List of Free Federal Government Cybersecurity Resources
Updated February 14, 2024

Federal Agencies

- **HHS**
  - **ASPR:** The U.S. Department of Health & Human Services' (HHS) Administration for Strategic Preparedness & Response's (ASPR) Technical Resources, Assistance Center, and Information Exchange (TRACIE) was created to meet the information and technical assistance needs of the healthcare industry.
  - **HC3:** The Health Sector Cybersecurity Coordination Center (HC3) is a leading resource for cybersecurity information sharing and technical-based resources to help mitigate cyber breaches.
  - **FDA:** The Food & Drug Administration (FDA) regulates medical devices.
  - **OCR:** The Office for Civil Rights (OCR) regulates HIPAA covered entities and oversees their compliance with privacy and security rules. More information on OCR is below.
- **CISA**
  - The Department of Homeland Security's (DHS) Cybersecurity Infrastructure and Security Agency (CISA) plays a lead role in strengthening cybersecurity resilience across the nation and sectors, investigating malicious cyber activity, and advancing cybersecurity alongside our democratic values and principles.
    - You can find our CISA Cheat Sheet here.
    - You can find CISA's stop ransomware website here.
    - You can sign up for DHS email updates and alerts here.
- **FBI**
  - The Federal Bureau of Investigation (FBI) oversees cybersecurity crimes. More information can be found below.
- **NIST:** The Department of Commerce's National Institute of Standards and Technology (NIST) develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies and the broader public. Their activities range from producing specific information that organizations can put into practice immediately to longer-term research that anticipates advances in technologies and future challenges.
    - You can find additional details on NIST and their cybersecurity resources here
    - NIST Security Configuration Checklists here
    - NIST National Vulnerability Database here

Healthcare and Public Health Sector Coordinating Council's Cybersecurity Working Group (HSCC CWG)

- Healthcare is one of the sixteen critical infrastructures in the country, and the HSCC CWG is the body recognized to represent our sector. It is comprised of more than 400 volunteers and works in collaboration with federal agencies.
- It is free to join, and we strongly encourage our members to do so. Fill out this form here to join.
- CHIME & AEHIS have members on their executive committee and we are active in many of their task groups.
- HSCC has great resources including:
    - Health Industry Cybersecurity Recommendations for Government Policy and Programs
    - Hospital Cyber Resiliency Landscape Analysis

        - Cybersecurity for the Clinician Video Series
        - HPH Sector Cybersecurity Framework Implementation Guide
    - The entire list of HSCC publications can be found here.

405(d) & the Healthcare Industry Cybersecurity Practices (HICP)

- **We strongly encourage you to become familiar with these tools.**
- The 405(d) Program and Task Group (under HSCC as described above) is a collaborative effort between industry and the federal government, which aims to raise awareness, provide vetted cybersecurity practices, and move organizations towards consistency in mitigating the current most pertinent cybersecurity threats to the sector.
- 405(d) gets its name from a provision in the Cybersecurity Information Sharing Act of 2015 which required HHS to work with industry to develop a voluntary set of best practices for the healthcare sector.
- These best practices are under the 405(d) Program – and are known as Health Industry Cybersecurity Practices (HICP):
    - HICP main document (2023 edition)
    - Technical Volume I (2023 edition) – small organizations
    - Technical Volume II (2023 edition) – medium and large organizations
- Find other resources from 405(d) here.
- **Why should you care?** A law passed in early 2021 specifically mentions 405(d) best practices and says that OCR may levy lower fines and shorter audits related to a breach if a HIPAA covered entity engaged in cybersecurity best practices tied to the NIST Cybersecurity Framework (CSF) – including 405(d) practices. Additionally, if you are using 405(d) best practices in your organization, you are on your way to implementing HHS' voluntary cybersecurity performance goals (CPGs). Learn more here.

Reporting a Medical Device Vulnerability

Reporting Cybersecurity Issues to the FDA: Healthcare providers can use the MedWatch voluntary report form for health professionals (Form 3500) to report a cybersecurity issue with a medical device. You can find FAQs on the MedWatch Voluntary Report here.

- You can find our Cheat Sheet on the Food and Drug Administration's (FDA) Final Guidance Document - Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions here.
- The FDA has a Fact Sheet on "The FDA's Role in Medical Device Cybersecurity – Dispelling Myths and Understanding."
- In collaboration with MITRE, the FDA has updated (Nov. 2022) the Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook, a resource to help healthcare organizations prepare for cybersecurity incidents. The playbook focuses on preparedness and response for medical device cybersecurity issues that impact device functions.
- The FDA's Playbook for Threat Modeling Medical Devices is an educational resource that discusses best practices for understanding basic threat modeling concepts and processes, and how to apply them to medical devices.
- To receive safety communications on medical devices, including cybersecurity-related safety communications, you can subscribe to FDA's Medical Devices Safety and Recalls emails here.
- If you are interested in a one-on-one conversation with the FDA concerning issues with a medical device, please contact the Public Policy team at policy@chimecentral.org and we will connect you.

Reporting a Cyber Incident

- **Contact the FBI:** See additional information below.
- **Contact CISA:** Please see our cheat sheet on free resources for the Cybersecurity & Infrastructure Security Agency (CISA).

Cybersecurity Resources

- **HHS, CISA, and HSCC:**
  - Healthcare and Public Health (HPH) Cybersecurity Toolkit here which consolidates resources from HHS, CISA, and HSCC.
- **NIST:**
  - Security Configuration Checklists here
  - National Vulnerability Database here
  - **HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework** here
- **Risk Assessments:**
  - OCR guidance on **risk assessment tools** here
  - The Office of the National Coordinator for Health Information Technology (ONC), in collaboration with OCR, developed a downloadable Security Risk Assessment (SRA) Tool to help guide you through the process – you can find it here.

HHS Office for Civil Rights (OCR) Data Breach Resources

- **Report a breach** to OCR here
- OCR **cybersecurity webpage** here
- OCR **ransomware guidance** here
  - OCR considers all ransomware attacks a breach; whether they must be reported depends on the situation.

Contacting Law Enforcement

- Learn more about what you can do to protect yourself from cyber criminals, how you can report cyber crime – including ransomware – and the FBI's efforts in combating evolving cyber threats.
- The FBI has specially trained cyber squads in each of their 56 field offices, working hand-in-hand with interagency task force partners.
- The rapid-response Cyber Action Team can deploy across the country within hours to respond to major incidents.
- The Internet Crime Complaint Center (IC3) website contains critical information, including tips and information about current crime trends.
  - Additionally, if you are a victim of a network intrusion, data breach, or ransomware attack – contact the IC3 and your local FBI field office as soon as possible.
  - You can file a report with the IC3 here; you can also report federal crimes to the FBI here.
  - You can find the IC3's Current Industry Alerts here.
- CyWatch (email them here) is the FBI's 24/7 operations center and watch floor, providing around-the-clock support to track incidents and communicate with field offices across the country.

Follow the Feds on Social Media

X (formerly Twitter)	LinkedIn
@ASPRgov	CISA
@ask405d	FBI Cyber Division
@CISACyber	HHS 405(d) Program
@HHSOCR	HHS ASPR
@FBI	Health Sector Cybersecurity Council (HSCC)
@NSACyber	