LIST OF FREE FEDERAL GOVERNMENT CYBERSECURITY RESOURCES

Updated June 2021

ALERTS

- **Sign up for HHS alerts:** https://asprtracie.hhs.gov/ The U.S. Department of Health & Human Services' (HHS) Assistant Secretary for Preparedness & Response's Healthcare Emergency Preparedness Information Gateway (or ASPR TRACIE) sends timely alerts on emergencies including cyber threats and information sharing.
- **HHS Twitter:** @PHEgov
- **Sign up for DHS alerts:** https://public.govdelivery.com/accounts/USDHSUSCERT/subscriber/new. The Department of Homeland Security (DHS) responds to incidents, analyzes data about emerging cyber threats and shares information with the industry.
- **DHS website:** https://www.cisa.gov/about-cisa
- **DHS on Twitter:** @USCERT_gov

REPORTING A DEVICE VULNERABILITY

Call the FDA: 1-866-300-4374. Contact the Food and Drug Administration (FDA) if you need to report a vulnerability impacting one of your devices. They have established an emergency hotline that can be used 24/7.Reports of impact on multiple devices should be aggregated on a system/facility level.

REQUESTING A FREE SCAN OF YOUR PUBLIC IP

Contact US-CERT: vulnerability_info@cisa.dhs.gov. The US-CERT's National Cybersecurity Assessment & Technical Services (NCATS) provides integrated threat intelligence and provides an objective third-party perspective on the current cybersecurity posture of the stakeholder's unclassified operational / business networks. There is no cost to use this service.

REPORTING A CYBER INCIDENT

- **Contact FBI 24/7 Cyber Watch (CyWatch):** +1 (855) 292-3937 or by e-mail at CyWatch@fbi.gov and contact your local Federal Bureau of Investigation (FBI) field office at www.fbi.gov/contact-us/field
- **Contact the Cybersecurity and Infrastructure Security Agency (CISA)** at Central@cisa.dhs.gov to report a threat or request incident response resources or technical assistance related to cyber threats.
- Utilize the **CISA Incident Reporting System** at https://us-cert.cisa.gov/forms/report. The CISA incident reporting system provides a secure web-enabled means of reporting computer security incidents to CISA. This system assists analysts in providing timely handling of your security incidents as well as the ability to conduct improved analysis. If you would like to report a computer security incident, please complete the form (link above). Please provide as much information as you can to answer the questions to allow CISA to understand your incident.
- See below resources for the FBI and Secret Service.

LIST OF FREE FEDERAL GOVERNMENT CYBERSECURITY RESOURCES

BREACH RESOURCES

- **OCR:** https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html HHS' Office for Civil Rights (OCR) requires covered entities to notify them if they discover a breach of unsecured protected health information.
- **OCR ransomware guidance:** https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf OCR considers all ransomware attacks a breach; whether they must be reported depends on the situation.
- **Risk assessment tools and information:** https://www.healthit.gov/providers-professionals/security-risk-assessment-tool
- **HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework:** https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf To help healthcare organizations covered by the Health Insurance Portability and Accountability Act (HIPAA) to bolster their security posture, HHS created a crosswalk that identifies "mappings" between the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the HIPAA Security Rule. The crosswalk also includes mappings to other commonly used security frameworks.
- **HHS quick response checklist & infographic for victims of cyberattack:** https://www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf and https://www.hhs.gov/sites/default/files/cyber-attack-quick-response-infographic.gif

CONTACTING LAW ENFORCEMENT

- **FBI:** On Sept. 15, 2016, the FBI issued a new alert (https://www.ic3.gov/media/2016/160915.aspx) on ransomware, "Ransomware Victims Urged to Report Infections to Federal Law Enforcement." The FBI urges victims to report ransomware incidents so they can better understand threats. The bureau also indicated that it does not support paying ransoms, however, "recognizes executives, when faced with inoperability issues, will evaluate all options to protect their shareholders, employees, and customers." The alert calls on victims to contact their local FBI office and / or file a complaint with the Internet Crime Complaint Center, at www.IC3.gov. This alert follows their bulletin (https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise) on ransomware published in April 2016.
- **Secret Service:** US Secret Service has an Electronic Crimes Task Force. Those interested in their help can locate their field office by going to https://www.secretservice.gov/contact/field-offices/. immediately to report a ransomware event and request assistance. These professionals work with state and local law enforcement and other federal and international partners to pursue cyber criminals globally and to assist victims of cybercrime.

LIST OF FREE FEDERAL GOVERNMENT CYBERSECURITY RESOURCES

RANSOMWARE

- **CISA**
  - Vulnerability scanning, web application scanning, phishing campaign assessment, and remote penetration testing services https://www.cisa.gov/cyber-hygiene-servicesSoftware
  - Ransomware Guidance and Resources https://www.cisa.gov/ransomware
  - Ransomware Guide https://www.cisa.gov/publication/ransomware-guide
  - Darkside Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks https://us-cert.cisa.gov/ncas/alerts/aa21-131a
- **FBI** Ransomware Webpage https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware
- **Engineering Institute** best practices for prevention and response https://insights.sei.cmu.edu/blog/ransomware-best-practices-for-prevention-and-response/
- **HHS**
  - Ransomware and HIPAA Fact Sheet https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf
  - HC3 Homepage https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html
  - 405(d) Ransomware Threat Flyer
  - 405(d) Spotlight Webinar-Ransomware
  - 405(d) Ransomware Cyber Awareness Flyer
- **NIST** Releases Tips and Tactics for Dealing with Ransomware https://www.nist.gov/news-events/news/2021/05/nist-releases-tips-and-tactics-dealing-ransomware
- **Ransomware Task Force** Combatting Ransomware Report https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf