Cybersecurity Best Practice Committee Resources for Small and Large Businesses

(v1.7 February 27, 2019)

Standards to follow

1. **National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations**
   https://doi.org/10.6028/NIST.SP.800-171r1

   The protection of Controlled Unclassified Information (CUI) while residing in nonfederal information systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully carry out its designated missions and business operations. This publication provides federal agencies with recommended requirements for protecting the confidentiality of CUI: when the CUI is resident in nonfederal information systems and organizations; when the information systems where the CUI resides are not used or operated by contractors of federal agencies or other organizations on behalf of those agencies; and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government wide policy for the CUI category or subcategory listed in the CUI Registry. The requirements apply to all components of nonfederal information systems and organizations that process, store, or transmit CUI, or provide security protection for such components. The CUI requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

   Organizations that have implemented or plan to implement the NIST Framework for Improving Critical Infrastructure Cybersecurity can use the mapping of the CUI security requirements to the security controls in NIST Special Publication 800-53 and ISO/IEC 27001 to locate the equivalent controls in the categories and subcategories associated with the core functions of the Framework: identify, protect, detect, respond, and recover. The security control mapping information can be useful to organizations that wish to demonstrate compliance to the CUI security requirements in the context of their established information security programs, when such programs have been built around the NIST or ISO/IEC security controls.

2. **20 Critical Security Controls** https://www.cisecurity.org/controls/ **enumerates the key security controls entities should start with**

3. **OWASP (Open Web Application Security Project)** https://www.owasp.org/index.php/Main_Page **OWASP focuses primarily on web security**

4. **OWASP Top 10 Critical Application Security Risks**
   https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

5. **NIST Special Publication 800-53A Assessing Security and Privacy Controls in Federal Information Systems and Organizations**
http://dx.doi.org/10.6028/NIST.SP.800-53Ar4

This publication provides a set of procedures for conducting assessments of security controls and privacy controls employed within federal information systems and organizations. The assessment procedures, executed at various phases of the system development life cycle, are consistent with the security and privacy controls in NIST Special Publication 800-53, Revision 4. The procedures are customizable and can be easily tailored to provide organizations with the needed flexibility to conduct security control assessments and privacy control assessments that support organizational risk management processes and that are aligned with the stated risk tolerance of the organization. Information on building effective security assessment plans and privacy assessment plans is also provided along with guidance on analyzing assessment results.

6. **NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations**
http://dx.doi.org/10.6028/NIST.SP.800-53r4

This publication provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors. The controls are customizable and implemented as part of an organization-wide process that manages information security and privacy risk. The controls address a diverse set of security and privacy requirements across the federal government and critical infrastructure, derived from legislation, Executive Orders, policies, directives, regulations, standards, and/or mission/business needs. The publication also describes how to develop specialized sets of controls, or overlays, tailored for specific types of missions/business functions, technologies, or environments of operation. Finally, the catalog of security controls addresses security from both a functionality perspective (the strength of security functions and mechanisms provided) and an assurance perspective (the measures of confidence in the implemented security capability). Addressing both security functionality and security assurance ensures that information technology products and the information systems built from those products using sound systems and security engineering principles are sufficiently trustworthy.

Organizations with knowledge sharing on practices and threat updates

7. **DHS -** https://www.dhs.gov/topic/cybersecurity

8. **FBI -** https://www.fbi.gov/investigate/cyber

9. **DSAC -** https://www.dsac.gov/topics/cyber-resources

10. **The Defense Industrial Base (DIB) Cybersecurity Program**
https://dibnet.dod.mil/portal/intranet/

11. **DLA Contractor Cyber Resources**
http://www.dla.mil/HQ/InformationOperations/Offers/Services/FIC/ContractorCyberResources/

Threat updates and analysis

12. **IACP Cybercenter -** http://www.iacpcybercenter.org/resource-center/cyber-threat-bulletins/

13. **DHS and US-CERT provide a number of very useful cyber news bulletins and alerts as part of the National Cyber Awareness System -** https://www.us-cert.gov/ncas

14. **SANS NewsBites** https://www.sans.org/newsletters/newsbites/ **is a "semiweekly high-level executive summary of the most important news articles that have been published on computer security during the last week."**

15. **POLITICO Morning Cybersecurity** http://www.politico.com/morningcybersecurity **offers "a daily briefing on politics and cybersecurity."**

16. **MS-ISAC Cyber Security Advisories** https://msisac.cisecurity.org/advisories/ **provides relevant news on cyber issues and threats. See more at:**
http://www.iacpcybercenter.org/resource-center/cyber-threat-bulletins/#sthash.Ydxznb3s.dpuf

17. **Surface Cybersecurity Awareness**
https://www.tsa.gov/for-industry/surface-transportation-cybersecurity-toolkit

18. **DHS Cyber Information Sharing and Collaboration Program (CISCP)** https://www.dhs.gov/ciscp

Collaboration, Sharing, and Compliance

19. **DHS Cyber Information Sharing and Collaboration Program (CISCP)**
https://www.dhs.gov/ciscp

    Information sharing is a key pillar of effective cybersecurity. By sharing information rapidly between the government and the private sector, network defenders are able to block cyber threats before damaging compromises occur. The Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) serves as the hub of information sharing activities for the Department to increase awareness of vulnerabilities, incidents, and mitigations. Within the NCCIC, the Cyber Information Sharing and Collaboration Program (CISCP) is DHS's flagship program for public-private information sharing and complements ongoing DHS information sharing efforts. In CISCP, DHS and participating companies share information about cyber threats, incidents, and vulnerabilities.

Information shared via CISCP allows all participants to better secure their own networks and helps support the shared security of CISCP partners. Further, CISCP provides a collaborative environment where analysts learn from each other to better understand emerging cybersecurity risks and effective defenses. CISCP is based upon a community of trust in which all participants seek mutual benefit from robust information sharing and collaboration. CISCP is free of charge and provides value to all members. Therefore, all companies with an interest in multi-directional cybersecurity information sharing and robust analytic collaboration between the government and the private sector should consider joining CISCP.

20. Department of Defense Cyber Crime Center's DoD-Defense Industrial Base (DIB) Collaborative Information Sharing Environment (DCISE)
http://www.dc3.mil/cyber-security/

The DoD Defense Industrial Base (DIB) Collaborative Information Sharing Environment (DCISE) serves as the single DoD focal point for receiving all cyber incident reporting affecting unclassified networks of DoD contractors from industry and other government agencies. DCISE also serves as the operational focal point for the voluntary Defense Industrial Base Cybersecurity (CS) Program under 32 Code of Federal Regulations part 236 designed to enhance and supplement DIB participants' capabilities to safeguard DoD information that resides on or transits DIB unclassified information systems. DCISE fosters a cyber threat information sharing partnership with DIB participants by performing cyber analysis, offering mitigation and remediation strategies, providing best practices and conducting analyst-to-analyst exchanges with DIB participants.

21. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
https://ics-cert.us-cert.gov/

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.

22. Information Sharing and Analysis Centers (ISACs)
https://www.nationalisacs.org/

Sector-based Information Sharing and Analysis Centers collaborate with each other via the National Council of ISACs. Formed in 2003, the NCI today comprises 24 organizations. It is a coordinating body designed to maximize information flow across the private sector critical infrastructures and with government. Critical infrastructure sectors and subsectors that do not have ISACs are invited to contact the NCI to learn how they can participate in NCI activities. Information Sharing and Analysis Centers help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards. ISACs collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency. ISACs reach deep into their sectors, communicating critical information far and wide and maintaining sector-wide situational awareness.

23. **Information Sharing and Analysis Organizations (ISAOs)**
https://www.dhs.gov/isao

America's cyber adversaries move with speed and stealth. To keep pace, all types of organizations, including those beyond traditional critical infrastructure sectors, need to be able to share and respond to cyber risk in as close to real-time as possible. Organizations engaged in information sharing related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States. However, many companies have found it challenging to develop effective information sharing organizations—or Information Sharing and Analysis Organizations (ISAOs). In response, President Obama issued the 2015 Executive Order 13691 directing the Department of Homeland Security (DHS) to encourage the development of ISAOs.

24. **INFRAGARD**
https://www.infragard.org/

InfraGard is a partnership between the FBI and members of the private sector. The InfraGard program provides a vehicle for seamless public-private collaboration with government that expedites the timely exchange of information and promotes mutual learning opportunities relevant to the protection of Critical Infrastructure. With thousands of vetted members nationally, InfraGard's membership includes business executives, entrepreneurs, military and government officials, computer professionals, academia and state
and local law enforcement; each dedicated to contributing industry specific insight and advancing national security.

25. **Defense Federal Acquisition Regulation Related Information**
252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012

26. **Webinar: What is NIST SP 800-171 and how does it apply to small business?**
https://cset.inl.gov/SitePages/Webinar2.aspx

27. **Controlled Unclassified Information (CUI) Registry**
http://www.archives.gov/cui/registry/category-list.html

- Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.

- Executive Order 13556 "Controlled Unclassified Information" (the Order), establishes a program for managing CUI across the Executive branch and designates the National Archives and Records Administration (NARA) as Executive Agent to implement the Order and oversee agency actions to ensure compliance. The Archivist of the United States delegated these responsibilities to the Information Security Oversight Office (ISOO).

- 32 CFR Part 2002 "Controlled Unclassified Information" was issued by ISOO to establish policy for agencies on designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI, self-inspection and oversight requirements, and other facets of the Program. The rule affects Federal executive branch agencies that handle CUI and all organizations (sources) that handle, possess, use, share, or receive CUI—or which operate, use, or have access to Federal information and information systems on behalf of an agency.

Training

28. Center for Development of Security Excellence (CDSE)
http://www.cdse.edu/catalog/cybersecurity.html

The Center for Development of Security Excellence (CDSE) is a nationally accredited, award-winning directorate within the Defense Security Service (DSS) located in Linthicum, MD. CDSE provides security education, training, and certification products and services to a broad audience supporting the protection of National Security and professionalization of the DoD security enterprise. Provides online courses related to cybersecurity topics such as risk management and phishing—that is, social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a fake website that requests information.

29. Federal Communications Commission's Cyberplanner
https://www.fcc.gov/cyberplanner

Information technology and high-speed Internet are great enablers of small business success, but with the benefits comes the need to guard against growing cyber threats. As larger companies take steps to secure their systems, less secure small businesses are easier targets for cyber criminals. In October 2012, the FCC re-launched Small Biz Cyber Planner 2.0, an online resource to help small businesses create customized cybersecurity plans. Use this tool to create and save a custom cyber security plan for your company, choosing from a menu of expert advice to address your specific business needs and concerns.

30. Information Assurance Support Environment Online Training
http://iase.disa.mil/eta/Pages/online-catalog.aspx

Provides training materials on cybersecurity awareness and technical and legal issues related to government network security, cybersecurity for organization leaders, and personal cybersecurity awareness. The cybersecurity awareness training is mandatory for all users of DOD furnished computers and holders of Common Access Cards.

31. National Initiative for Cybersecurity Education (NICE)
http://csrc.nist.gov/nice/index.htm

The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST), is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. The mission of NICE is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. NICE fulfills this mission by coordinating with government, academic, and industry partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals helping to keep our Nation secure.

32. Small Business Community (SBC) Computer Security Workshops
http://csrc.nist.gov/groups/SMA/sbc/workshops.html

NIST, in co-sponsorship with the Small Business Administration (SBA) and the Federal Bureau of Investigation (FBI), conducts workshops on information security threats and solutions. Given NIST's expertise in the area of information security, SBA's extensive network built to help small businesses start, grow, and succeed, and the FBI's InfraGard program's frontline view of information security threats, the workshops resulting from this partnership deliver information security training to the small business community like no other. These workshops are especially designed for small businesses and not-for-profit organizations. Attendees will have the opportunity to explore practical tools and techniques that can help them to assess, enhance, and maintain the security of their systems and information.

33. U.S. Computer Emergency Readiness Team's Resources for Business
https://www.us-cert.gov/ccubedvp/business

1. How to protect your business from intentional attacks or unintentional damage by well meaning employees?
2. How to guard against the embarrassment, legal liability or decreased productivity of security breaches?
3. How to evaluate security tools and techniques based on your needs?

The resources are available to businesses and aligned to the five Cybersecurity Framework Function Areas. Some resources and programs align to more than one Function Area.
U.S. Small Business Administration's Cybersecurity for Small Businesses
https://www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses

This self-paced training exercise provides an introduction to securing information in a small business. Topics include: Defining cybersecurity; Explaining the importance of securing information through best cybersecurity practices; Identifying types of information that should be secured; Identifying the types of cyber threats; Defining risk management; and Listing best practices for guarding against cyber threats.

Appendix: Federal Trade Commission & Federal Communications Commission Intros to Cybersecurity for Small Businesses

1. The Federal Trade Commission - Cybersecurity for Small Business (https://www.fcc.gov/general/cybersecurity-small-business)
2. The Federal Communications Commission's 10 Cybersecurity Tips for Small Business List (https://www.fcc.gov/general/cybersecurity-small-business)
3. The U.S. Small Business Administration's "10 Cybersecurity Mistakes Your Small Business Cannot Afford to Make" WebinarThe Federal Communications Commission Cyberplanner (https://www.youtube.com/watch?v=KLrnI5ZEl9Y&feature=youtu.be)