

ABOUT THIS GUIDE

The Cybersecurity Resources Road Map is designed to help critical infrastructure small and midsize businesses identify useful cybersecurity resources to meet their needs.

The road map comprises *four tiers* and *two questions* in each tier. Each question introduces a topic and a few related resources.

The tiers reflect degrees of cybersecurity sophistication. In general, companies that have well-developed cyber capabilities will find the resources in the higher tiers most appropriate, while companies that have less sophisticated cyber capabilities will likely focus on the lower tiers.

However, the best approach is to consider all the questions and all the resources in view of the organization's objectives and assessment of risk.

ADDITIONAL RESOURCES

The U.S. Department of Homeland Security's National Protection and Programs Directorate leads the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure. To learn about additional resources beyond those recommended in this guide, visit: <https://www.dhs.gov/topic/cybersecurity>.

The tier structure presented in this guide generally reflects the Cybersecurity Framework, which was developed by the National Institute of Standards and Technology. For information, visit: <https://www.nist.gov/cyberframework>.

CYBERSECURITY RESOURCES ROAD MAP

A GUIDE FOR CRITICAL INFRASTRUCTURE

SMALL AND MIDSIZE BUSINESSES



Homeland Security

TIER 1

Have you communicated the importance of cybersecurity to your business?

- **Cybersecurity Tools** (SBA)
<https://www.sba.gov/managing-business/cybersecurity>
- **Small & Midsize Business Cybersecurity Toolkit** (DHS)
<https://www.us-cert.gov/ccubedvp/smb>
- **Cybersecurity Tip Sheets** (DHS)
<https://www.us-cert.gov/ncas/tips>

Has your business begun to follow basic cybersecurity best practices?

- **Start with Security: A Guide for Business** (FTC)
<https://www.ftc.gov/>
(Run a search for title of document)
- **Small Business Information Security: The Fundamentals** (NISTIR 7621)
<https://www.nist.gov/>
(Run a search for title of document)
- **Factsheet: Cyber Incident Reporting** (DHS)
<https://www.dhs.gov/cyber>
(Run a search for "cyber incident reporting")

TIER 2

Are you implementing a leadership-driven, company-wide cybersecurity program?

- **Cybersecurity Framework** (NIST)
<https://www.nist.gov/cyberframework>
- **Cybersecurity Framework Guidance** (DHS)
<https://www.us-cert.gov/ccubedvp/cybersecurity-framework>
- **Cybersecurity Education and Training Catalog** (DHS)
<https://niccs.us-cert.gov/training>

Have you integrated cybersecurity with risk management processes?

- **Managing Information Security Risk** (NIST 800-39)
<https://www.nist.gov/>
(Run a search for "800-39")
- **Guide for Conducting Risk Assessments Rev. 1** (NIST 800-30)
<https://www.nist.gov/>
(Run a search for "800-30")
- **Threat Alerts, Bulletins, Advisories** (DHS)
<https://www.us-cert.gov/ncas>
and <https://ics-cert.us-cert.gov>

TIER 3

Are you evaluating your cybersecurity posture and capabilities?

- **Cybersecurity Assessments** (DHS)
(Provided to critical infrastructure on a priority basis)
Call 888-282-0870 or email nccicustomerservice@hq.dhs.gov or cyberadvisor@hq.dhs.gov
- **Cyber Tabletop Exercise for SMBs** (DHS)
Call 888-282-0870 or email nccicustomerservice@hq.dhs.gov

Are you participating in an information sharing forum to gain insights and strategies?

- **Information Sharing and Analysis Centers** (National Council of ISACs)
<https://www.nationalisacs.org/>
- **Information Sharing and Analysis Organizations** (ISAO Standards Organization)
<https://www.isao.org/>
- **Secure Information Sharing Portal** (DHS)
Call 888-282-0870 or email nccicustomerservice@hq.dhs.gov

Note: Professional business organizations also offer cyber information sharing opportunities.

TIER 4

Have you trained your staff to prevent, detect, and respond to cyber incidents?

- **Industrial Control System Training Classroom and online courses** (DHS)
<https://ics-cert.us-cert.gov>
- **Cybersecurity Education and Training Catalog** (DHS)
<https://niccs.us-cert.gov/training>
- **NICE Cybersecurity Workforce Framework** (NIST)
<https://niccs.us-cert.gov/workforce-development>
(Click on Training)

Are you utilizing cyber defense technologies to support your operation?

- **Automated Indicator Sharing** (DHS)
(Threat indicator exchange in near real-time)
<https://www.dhs.gov/ais>
- **Cyber Information Sharing and Collaboration Program** (DHS)
(Threat indicator exchange plus trusted analysis)
<https://www.dhs.gov/ciscp>
- **Enhanced Cybersecurity Services** (Commercial intrusion prevention capabilities)
<https://www.dhs.gov/enhanced-cybersecurity-services>

Note: ISACs and ISAOs provide access to cyber defense technologies as well.