Small Business Development Center Cyber Strategy

March 15, 2019

Homeland Security

U.S. Small Business Administration

Joint Foreword from the Secretary of the U.S. Department of Homeland Security and the Administrator of the U.S. Small Business Administration

March 15, 2019

We are pleased to submit the Small Business Development Center Cyber Strategy, jointly prepared by the U.S. Department of Homeland Security (DHS) and the U.S. Small Business Administration (SBA) in consultation with the National Institute of Standards and Technology (NIST) and America's Small Business Development Centers (SBDCs).

This strategy has been compiled pursuant to the requirements in Section 1841 of the *National Defense Authorization Act of Fiscal Year 2017* (Pub. L. No. 114-328) and was created to help small and medium sized businesses enhance their cyber planning and risk management.

Pursuant to Congressional requirements, this strategy is being provided to the following Members:

The Honorable Bennie G. Thompson
Chairman, House Committee on Homeland Security

The Honorable Mike Rogers
Ranking Member, House Committee on Homeland Security

The Honorable Nydia Velázquez
Chairman, House Committee on Small Business

The Honorable Steve Chabot
Ranking Member, House Committee on Small Business

The Honorable Ron Johnson
Chairman, Senate Committee on Homeland Security and Governmental Affairs

The Honorable Gary C. Peters
Ranking Member, Senate Committee on Homeland Security and Governmental Affairs

The Honorable Marco Rubio
Chairman, Senate Committee on Small Business and Entrepreneurship

The Honorable Ben Cardin
Ranking Member, Senate Committee on Small Business and Entrepreneurship

Should you need additional assistance, please have your staff contact the DHS Office of Legislative Affairs on (202) 447-5890.

Sincerely,

Kirstjen M. Nielsen
Secretary
U.S. Department of Homeland Security

Linda E. McMahon
Administrator
U.S. Small Business Administration

Executive Summary

There are nearly 30.2 million small businesses in the United States that employ 47.5 percent of the Nation's workforce.[1] A small business is typically defined as a company with fewer than 500 employees, according to the U.S. Small Business Administration (SBA) Table of Small Business Size Standards.[2] However, the SBA notes that in some sectors, small businesses employ up to 1,500 employees or are defined by annual receipts.[3] Small businesses often use information technology to maintain operations, protect customer data, and secure financial and intellectual property. A cyberattack can severely harm small business operations and reduce consumer confidence. Over 85 percent of small business owners fear cyberattacks and feel unprepared to handle one. Over 85 percent of small business owners also feel they have inadequate resources to protect themselves.[4]

The SBA's nationwide network of Small Business Development Centers (SBDCs) provides business and economic development assistance to small business stakeholders to promote their growth, expansion, and innovation. Given today's landscape of ever-increasing cybersecurity threats, SBDCs are acutely poised to help small businesses prepare for, respond to, and recover from cybersecurity threats through training, counseling, and risk management tools designed to mitigate the risks facing small businesses.

In December 2016, Congress released the *National Defense Authorization Act for Fiscal Year (FY) 2017* requiring the U.S. Department of Homeland Security (DHS) and SBA to develop a Cyber Strategy for SBDCs. DHS and SBA developed the SBDC Cyber Strategy with the America's Small Business Development Centers (ASBDCs)[5] and the National Institute of Standards and Technology[6] (NIST). The purpose of this strategy is to recommend actions to advance the capabilities of SBDCs to provide cybersecurity support to U.S. small businesses. The findings and recommendations form a starting point for enhancing and integrating existing federal programs, projects, and activities to support SBDCs as they work to extend cyber support to U.S. small businesses. In addition, this strategy supplies information on available federal tools and resources to immediately implement and strengthen small businesses' cybersecurity. Recommendations contained in this strategy define ways to use current federal resources to

---

[1] https://www.sba.gov/sites/default/files/Whats-New-With-Small-Business-2018.pdf

[2] https://www.sba.gov/contracting/getting-started-contractor/make-sure-you-meet-sba-size-standards/table-small-business-size-standards%20%20

[3] Under Section 3 of the Small Business Act, a "small business concern" is deemed to be an enterprise that: (i) is independently owned and operated; (ii) is not dominant in its field of operation; and (iii) is within the applicable size standards for its industry.

[4] The America's Small Business Development Centers surveyed Small Business Development Centers and small business on cybersecurity topics for this strategy (Section III)

[5] America's Small Business Development Centers (SBDC) is the association that represents America's nationwide network of SBDCs and is the most comprehensive small business assistance network in the United States and its territories. They offer no-cost business consulting and low-cost business training, through local SBDCs which can be found at https://americassbdc.org/.

[6] On August 14, 2018 Congress passed the NIST Small Business Cybersecurity Act. This Act requires NIST to disseminate cyber defense resources for small businesses by creating a set of guidelines for basic security measures that should be easy to follow and implement affordably. It also creates guidelines for making security best practices a required component of corporate training and workplace culture more can be found at https://www.congress.gov/bill/115th-congress/senate-bill/770.

improve and extend the support services of SBDCs, as they advise and assist with small business cyber planning and risk management.

Subject to available resources and approval, the following recommendations identify how SBDCs can connect small businesses with federal programs, projects, and activities to improve access to high-quality cyber support:

- Centralize cybersecurity information and resources on the SBA website to be easily accessible by SBDC advisors and businesses;
- Provide a needs/risk-based resource mapping tool;
- Compile a digital directory of resources;
- Provide access to existing cyber training resources;
- Extend advisor expertise on cybersecurity across SBDCs through training;
- Expand the cybersecurity subject matter expertise community of practice;
- Produce and provide access to information sharing training for SBDCs;
- Produce and provide access to guidebooks for small businesses; and,
- Develop promotional campaign and research cycle.

Small businesses are fully cognizant that they need to take additional measures to protect against potential cyber threats. DHS and SBA recognize the opportunity to strengthen small business cybersecurity by working with the SBDCs. This strategy shares information on what SBDCs need to consistently connect their small business clients to federal cybersecurity programs, projects, and activities. Together DHS, SBA, and SBDCs will strengthen small businesses' cyber defense by overcoming the common cybersecurity challenges of information sharing and access to government resources, and by making it easier for small businesses to address the full cybersecurity risk management lifecycle.

Small Business Development Center Cyber Strategy

Table of Contents

I. Legislative Language

SEC. 1841. SMALL BUSINESS DEVELOPMENT CENTER CYBER STRATEGY AND OUTREACH.

(a) SMALL BUSINESS DEVELOPMENT CENTER CYBER STRATEGY.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Administrator of the Small Business Administration and the Secretary of Homeland Security shall work collaboratively to develop a cyber strategy for small business development centers to be known as the "Small Business Development Center Cyber Strategy."

(2) CONSULTATION.—In developing the strategy under this subsection, the Administrator of the Small Business Administration and the Secretary of Homeland Security shall consult with entities representing the concerns of small business development centers, including any association recognized under section 21(a)(3)(A) of the Small Business Act (15 U.S.C. 648(a)(3)(A)).

(3) CONTENT.—The strategy required under paragraph (1) shall include, at minimum, the following:

(A) Plans for allowing small business development centers (hereafter in this paragraph referred to as "SBDCs") to access existing cyber programs of the Department of Homeland Security and other appropriate federal agencies to enhance services and streamline cyber assistance to small business concerns.

(B) To the extent practicable, methods for providing counsel and assistance to improve a small business concern's cybersecurity infrastructure, awareness of cyber threat indicators, and cyber training programs for employees, including—

(i) working to ensure individuals are aware of best practices in the areas of cybersecurity, awareness of cyber threat indicators, and cyber training;

(ii) working with individuals to develop cost-effective plans for implementing best practices in these areas;

(iii) entering into agreements, where practical, with Information Sharing and Analysis Centers or similar entities that share cyber information to gain an awareness of actionable cyber threat indicators that may be beneficial to small business concerns; and

(iv) providing referrals to area specialists when necessary.

(C) An analysis of—

(i) how Federal Government programs, projects, and activities can be leveraged by SBDCs to improve access to high-quality cyber support for small business concerns;

(ii) additional resources SBDCs may need to effectively carry out their role; and

(iii) how SBDCs can leverage existing partnerships and develop new partnerships with Federal, State, and local government entities as well as private entities to improve the quality of cyber support services to small business concerns.

(4) DELIVERY OF STRATEGY.—Not later than 1 year after the date of enactment, the Small Business Administrator and the Secretary of Homeland Security shall submit to the Committees on Homeland Security and Small Business of the House of Representatives and the Committees on Homeland Security and Governmental Affairs and Small Business and Entrepreneurship of the Senate the Small Business Development Center Cyber Strategy developed under paragraph (1).

(5) DEFINITIONS.—In this subsection, the following definitions shall apply:

(A) CYBER THREAT INDICATOR.—The term "cyber threat indicator" has the meaning given such term in section 227(a) of the Homeland Security Act of 2002 (6 U.S.C. 148(a)).

(B) SMALL BUSINESS DEVELOPMENT CENTER.—The term "small business development center" has the meaning given such term in section 3 of the Small Business Act (15 U.S.C. 632).

(ii) CYBERSECURITY OUTREACH FOR SMALL BUSINESS DEVELOPMENT CENTERS.—Section 227 of the Homeland Security Act of 2002 (6 U.S.C. 148) is amended—

(1) by re-designating subsection (l) as subsection (m); and

(2) by inserting after subsection (k) the following new subsection:

"(l) CYBERSECURITY OUTREACH.—

"(1) IN GENERAL.—The Secretary may leverage small business development centers to provide assistance to small business concerns by disseminating information on cyber threat indicators, defense measures, cybersecurity risks, incidents, analyses, and warnings to help small business concerns in developing or enhancing cybersecurity infrastructure, awareness of cyber threat indicators, and cyber training programs for employees.

"(2) DEFINITIONS.—For purposes of this subsection, the terms 'small business concern' and 'small business development center' have the meaning given such terms, respectively, under section 3 of the Small Business Act."

II. Background

There are 30.2 million small businesses in the United States that employ 47.5 percent of the Nation's workforce.[7] Small businesses are increasingly reliant on information technology (IT). Protecting customer data, along with securing financial and intellectual property, is critical to maintaining operations and consumer confidence. However, over 85 percent of small business owners fear cyberattacks, and feel that they are unprepared for and have inadequate resources to protect themselves against such attacks.[8]

The U.S. SBA nationwide network of SBDCs provide business and economic development assistance to small business stakeholders to promote their growth, expansion, and innovation. SBDCs are hosted by leading universities and state economic development agencies and provide one-on-one advisement to small business owners seeking assistance on a broad range of business and technical areas. Given today's landscape of ever-increasing cybersecurity threats, SBDCs are acutely poised to help small businesses prepare for, and recover from, cybersecurity threats through training, counseling, and risk management tools designed to mitigate the risks facing small businesses.

On December 23, 2016, Congress released the *National Defense Authorization Act (NDAA) for FY 2017*. In Subtitle E – Improving Cyber Preparedness for Small Businesses, DHS and SBA were tasked to develop a cyber strategy for SBDCs to be known as the *Small Business Development Center Cyber Strategy*.

This SBDC Cyber Strategy establishes a clear vision with recommended actions for advancing SBDC capabilities and public-private sector partnerships to improve the cybersecurity posture of the small business community. These actions would allow SBDCs to access federal cybersecurity resources and make cybersecurity part of their mission.

The conclusions and recommendations contained in this strategy specifically address: (1) the way SBDCs should access DHS and other federal cyber programs; (2) proposed methods for providing counsel to help small businesses; (3) how Federal Government programs, projects, and activities can be leveraged by SBDCs; and (4) existing Federal, state, and local government partnerships can be leveraged to support the activities described in this strategy.

2.1 Methodology

DHS and SBA led the development of the *SBDC Cyber Strategy* in coordination with ASBDC and the NIST, and formed a taskforce to:

1. Conduct open-source research to identify Federal Government programs, projects, and activities applicable to small businesses;
2. Administer two nationwide surveys to relevant stakeholders; and,
3. Assess SBDCs' use of federal partnerships.

Section V of this strategy provides recommended plans and methods as required by Section (a)(3)(A) and (a)(3)(B) of the *NDAA for FY 2017*. Those plans and methods are derived from the

[7] https://www.sba.gov/sites/default/files/Whats-New-With-Small-Business-2018.pdf

[8] The America's Small Business Development Centers surveyed SBDCs and small business on cybersecurity topics for this strategy (Section III).

findings identified in Section IV: Analysis, as required by Section (a)(3)(C) of the *NDAA for FY 2017*. The gathered information supports the analysis discussed in Section III: Research.

2.2 Existing DHS and SBA Capabilities

Section 1841 of the *NDAA for FY 2017* presents DHS and SBA with an opportunity to articulate a strategic vision for building upon current U.S. federal partnerships and outreach to SBDCs and the small business community. DHS engages with small businesses through a variety of programs and offerings such as technical alerts and products, the Cyber Information Sharing and Collaboration Program (CISCP) and the Automated Information Sharing (AIS) program. CISCP provides no-cost information sharing capabilities, including venues on a monthly basis (webinars) as well as quarterly live analyst-to-analyst exchanges that are invaluable in sharing tactics, techniques, and procedures specifically on vulnerabilities and trends that can be applicable to small and mid-size businesses (SMBs). Additionally, the AIS program is a forum for exchanging and processing cyber threat indicators and defensive measures for SMBs. At present, roughly 40 percent of the entire non-federal AIS stakeholders are from SMBs.

The DHS Cybersecurity and Infrastructure Agency (CISA) is well positioned to implement the recommendations described in this strategy. CISA has provided a range of programs to support the cyber resiliency of public and private sector stakeholders, including the SMB Roadshow and the SMB Toolkit. Current efforts include partnership activities, technical assistance, educational services and outreach to critical infrastructure, SMBs, and state, local, tribal, and territorial (SLTT) governments.

SBA is also well positioned to implement the recommendations in this strategy in partnership with DHS. SBA's Partner Training Portal provides SBDCs, the SCORE Association[9], and Womens' Business Centers direct access to online training on small business issues – this platform can be leveraged to meet the cybersecurity training needs of the small business community. In addition, SBA partners with ASBDC and other federal organizations, and collaborates with SBDCs (and hence, the entire network of SBDC advisors), to support small business interests.

III. Research

In the preparation of this strategy, DHS and SBA conducted four data collections to support the analysis required in Section (a)(3)(C) of the NDAA for FY 2017.

- The analysis of "how Federal Government programs, projects, and activities can be leveraged by SBDCs to improve access to high-quality cyber support for small business concerns" was supported by information gathered about the existing Federal Government cybersecurity resources to address small business concerns (see Section 3.1 *Existing U.S. Federal Government Cybersecurity Resources for Small Business*).
- The analysis of "additional resources that SBDCs may need to effectively carry out their role" was supported by two national surveys conducted to assess the cybersecurity needs

[9] SCORE is the Nation's largest network of volunteer, expert business mentors, with more than 10,000 volunteers in 300 chapters. As a resource partner of the SBA, SCORE has helped more than 10 million entrepreneurs through mentoring, workshops and educational resources since 1964 which can be found at https://www.score.org/.

of small businesses and SBDCs (see Section 3.2 *Cybersecurity Needs of Small Business and SBDCs*).

- The analysis of "how SBDCs can leverage existing partnerships and develop new partnerships with SLTTs as well as private sector entities to improve the quality of cyber support services to small business concerns" was supported by information gathered about existing SBDC partnerships and use of federal programs.

Continued research is one of the recommendations contained in Section V of this strategy. The research contained in this section represents an initial snapshot of an evolving landscape. The following findings and the subsequent analysis and recommendations serve as a first step towards creating an overarching strategic vision.

3.1 Existing U.S. Federal Government Cybersecurity Resources Cybersecurity Resources for SMBs

DHS, SBA, and NIST conducted open-source research and compiled a preliminary list of cybersecurity resources to help small businesses address their cybersecurity concerns.

DHS is the federal lead for defending the cybersecurity of our Nation's critical networks. DHS coordinates a broad range of cybersecurity strategies and offers numerous resources useful to the small business community.

The Federal Government resources identified 46 cybersecurity programs, projects, and activities available to small businesses (Appendix E: Examples of Available Resources). This sample was used by DHS and SBA to identify gaps in the Federal Government's current cybersecurity offerings and informed the recommendations in this strategy.

Some of the programs identified in Appendix E were created specifically for small businesses, while others serve a larger critical infrastructure audience. Many of the resources in Appendix E are found online and the SBDCs can easily distribute the information at little to no cost to them or the small business community.

The resources presented in Appendix E have been grouped by the NIST Cybersecurity Framework's (The Framework) five core functions: Identify, Protect, Detect, Respond, and Recover. Together, these functions provide a high-level, strategic view of an organization's cybersecurity risk management lifecycle. The Framework Core also identifies the underlying key categories and subcategories for each function, and matches them with existing standards, guidelines, and practices for each subcategory.

3.2 Small Business and SBDCs Cybersecurity Needs

In order to solicit feedback on the cybersecurity needs of small businesses and SBDCs, ASBDC conducted 2 simultaneous nationwide 60 day surveys: 1 external survey directed to small business community stakeholders and 1 internal survey focused on the SBDC leaders.

The first external survey collected feedback from small business owners and operators on their cybersecurity concerns. Small business owners shared that their greatest needs were in the area of education, assistance, and where they perceived their company is most vulnerable. The survey

also captured the degree to which small businesses are aware of, use, or could benefit from federal programs, projects, and activities.

The second internal survey solicited SBDC leaders' input on cybersecurity issues and concerns as they observe in the greater small business community. Like the first survey, the findings provided insight regarding the importance and availability of cyber resources to SBDC programs across the country. The survey captured the degree to which SBDCs are prepared to provide cybersecurity consultation and support to address small business concerns. The survey results and a comprehensive analysis of the findings are presented in Sections 3.2.1 and 3.2.2 below.

3.2.1 Small Business Community Survey (External Survey).

The external survey was sent out through the SBDC networks to small business owners and operators who voluntarily provided responses. This survey received inputs from 398 respondents spanning across 22 states. Small businesses were asked a series of 16 questions designed to identify the areas where they felt most at risk of a cyberattack and where their businesses are lacking in cyber defense resources.

Of the 398 respondents, over 93 percent indicated they do not believe small businesses generally have adequate resources to respond to a cyber incident. In addition, over 88 percent of respondents felt their businesses were at risk of cyberattacks (Figure 2).

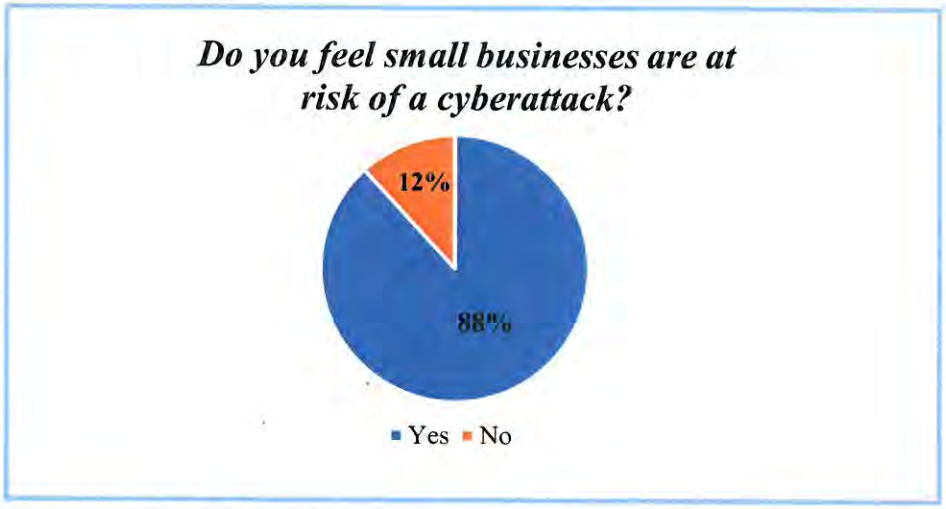

Figure 1: Small Businesses Feelings on Risk of a Cyberattack

The survey furthered showed that the small business owners' primary focus is on viruses, malware, and ransomware infiltrating their systems (Figure 3).

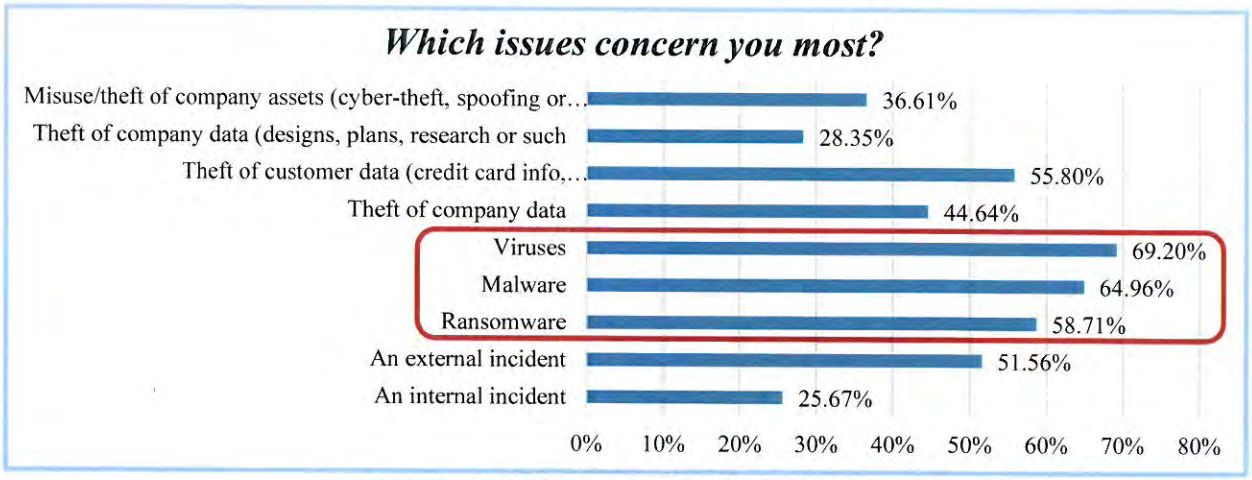

Figure 2: Small Businesses Most Concerned Issues

The responses indicated that 85 percent of small business owners do not feel they have adequate resources to prepare for cyberattacks (Figure 4).

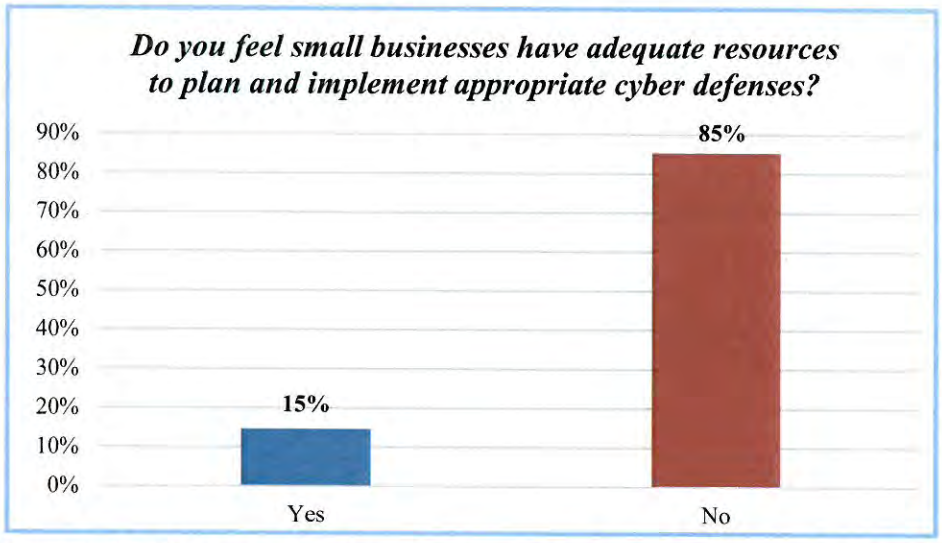

Figure 3: Small Businesses on Adequate Resources to Plan and Implement Cyber Defenses

Small business owners also identified a broad range of resources and assistance that would be most important for their small businesses to address cybersecurity concerns. The highest ranked resources were training for managers and direct help with planning were identified as important by more than half of respondents (Figure 5).

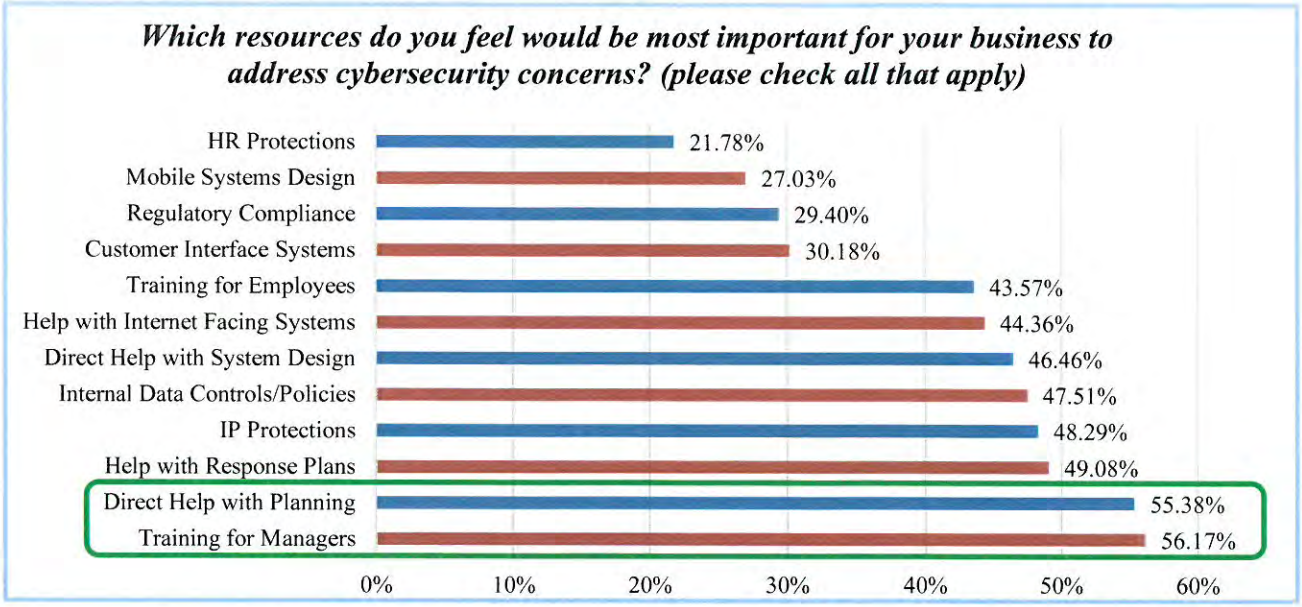

Figure 4: Resources and Assistance Most Important to Address Cybersecurity Concerns

The survey further demonstrated that the highest ranked forms of assistance were one-on-one counseling, online tools, and webinars (Figure 6).

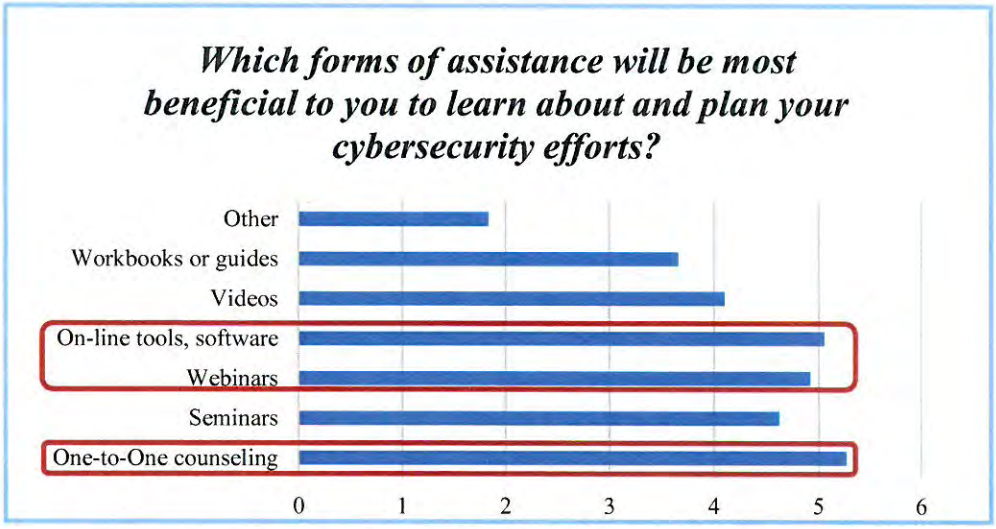

Figure 5: Forms of Assistance Most Beneficial for Cybersecurity Efforts

Despite the expressed need for resources to address cyber concerns, 70 percent of respondents said they were not aware of the available resources (Figure 7), and only 8 percent indicated they looked for resources from the Federal Government (Figure 8).

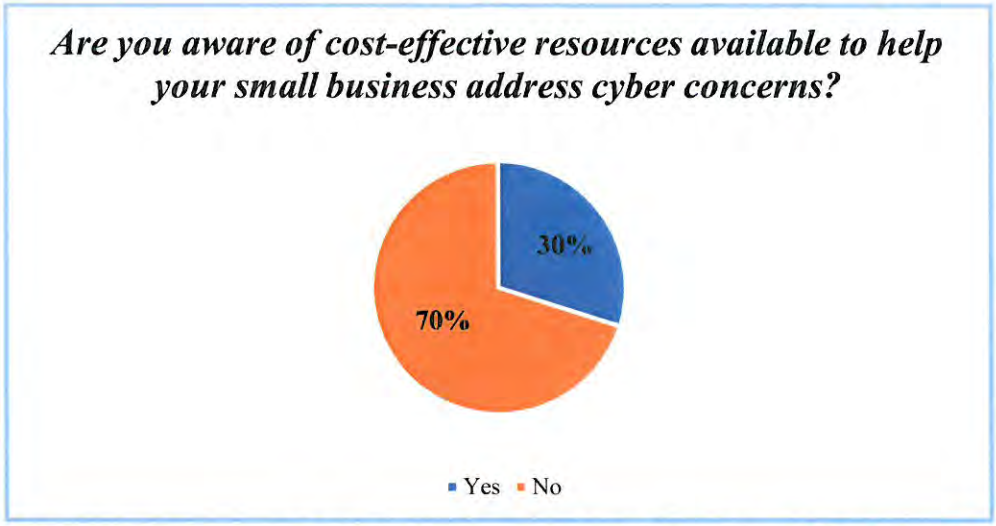

Figure 6: Awareness of Cost-Effective Resources Available to Address Cyber Concerns

Figure 7: Resources Sought to Address Cybersecurity Concerns

More than half of respondents indicated they need skills in small business defensive and response strategies. Over 40 percent indicated a need for training seminars, webinars, and workshops and request support with business planning and understanding the cost of cybersecurity (Figure 9).

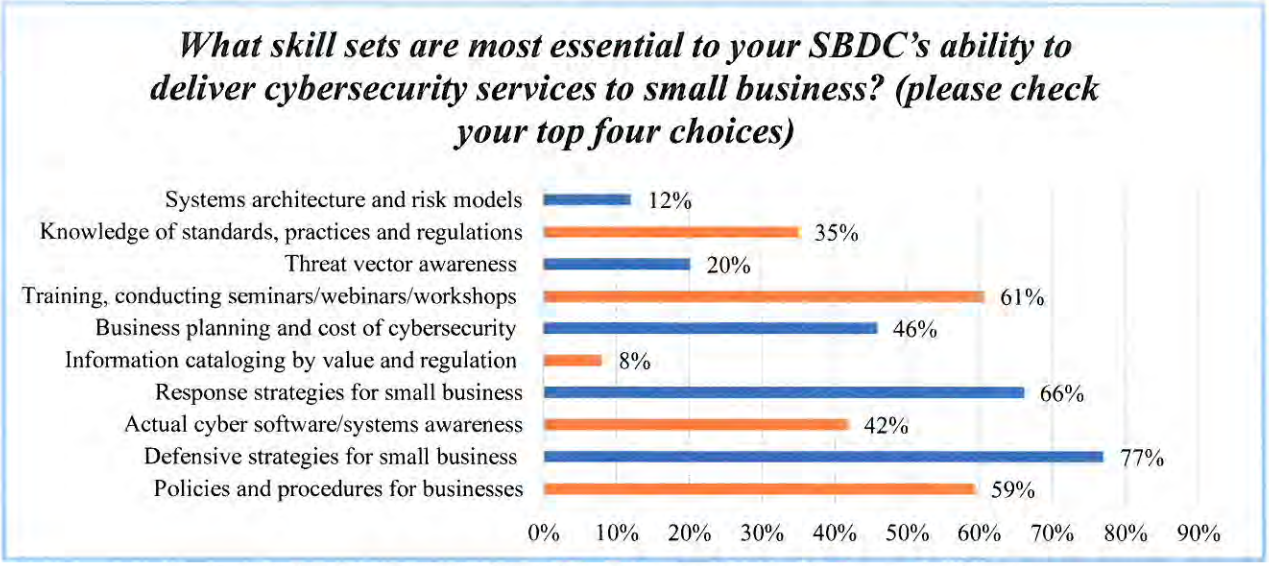

Figure 8: Most Essential Skills Sets Needed to Deliver Cybersecurity Services

3.2.2 SBDC Survey (Internal Survey)

The internal survey measured SBDC perceptions of their small business clients' cybersecurity needs. SBDC networks survey received feedback from 75 respondents with a 95 percent response rate. More than 40 percent of respondents said their respective networks were very concerned about cybersecurity for small businesses; however, more than 50 percent of respondents said their efforts to address cybersecurity are only sometimes or never supported. Most SBDCs (65 percent) had not conducted any cybersecurity workshops or seminars.

The survey asked about the importance of cyber resources and experts to SBDC programs across the country. Over 80 percent of respondents indicated that it is very important to have access to cybersecurity advisements, trainings, and experts, and gave these topics a seven on a 10-point scale in the survey. On a 10-point scale, 80 percent of respondents scored seven or greater for cybersecurity advisement/training resources and 85 percent scored seven or greater for cybersecurity advisement/training experts (rating them as very important).

Despite the expressed importance of cybersecurity advisement/training experts, only 56 percent of SBDCs have staff with expertise or interest in cybersecurity, and 73 percent said they do not have trained staff on small business cybersecurity for clients. About 51 percent of respondents rated their readiness to deliver cybersecurity advisement/training on the lower half of a 10-point scale.

The internal survey measured SBDC perceptions of their small business clients' cybersecurity needs. Awareness is at the top of the list, followed closely by defining needs and training. Despite the expressed importance of cybersecurity training, 84.93 percent of responding SBDCs have not created workbooks or guides for small businesses, and only 26.32 percent have drawn upon resources from federal agencies.

SBDCs identified advisor training, client materials (workbooks, software, etc.), and fiscal support as the top three identified needs in developing programmatic readiness or planning for small business cybersecurity needs. The top three skill sets identified can be categorized under defensive strategies, response strategies, and training (Figure 10).

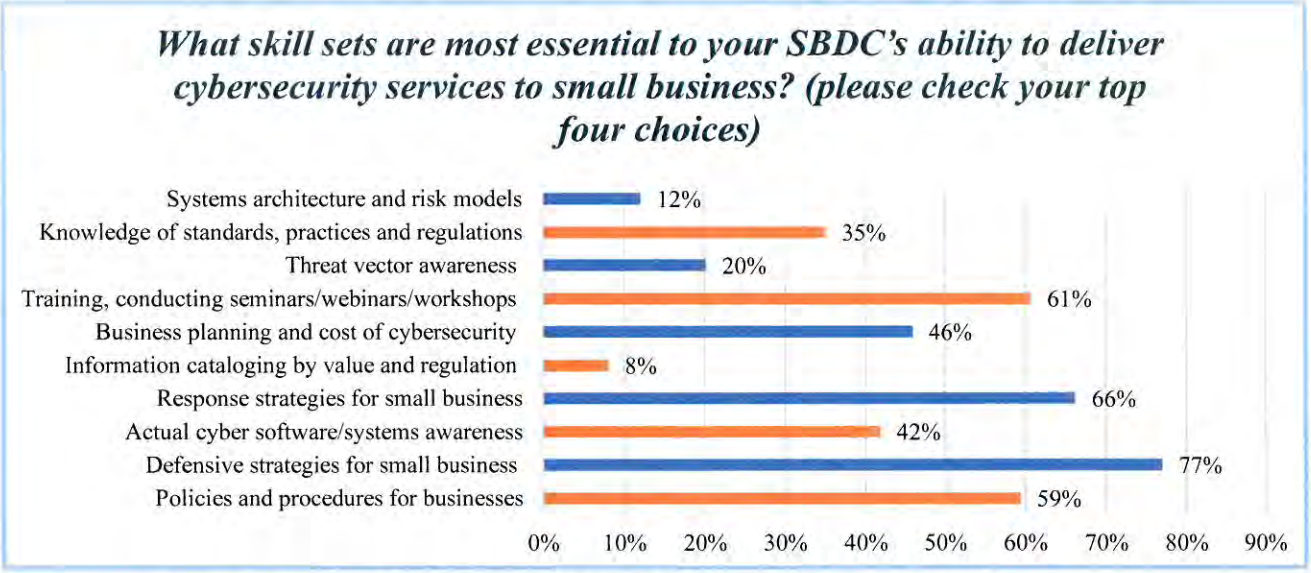

Figure 9: Skill Sets Most Essential to Deliver Cybersecurity Services to Small Businesses

3.3 Leveraging Existing Partnerships

SBDCs currently access a wide array of federal programs to support the needs of their small business customers. SBDCs are hosted by leading universities and state economic development agencies. They are funded in part through a partnership with SBA, and provide assistance to small businesses and entrepreneurs throughout the United States and its territories. SBDCs provide one-on-one advisement to small business owners seeking assistance with a broad range of business and technical areas. Those services often include training for managers and direct help with planning that identifies issues—not always obvious to clients—and provide responsive training or guidance. SBDCs assist small businesses in developing an understanding of these issues, codifying the need, and helping build capabilities, often through online training courses and seminars.

ASBDC reviewed all 63 lead SBDC websites in order to explore how SBDCs can leverage existing partnerships and develop new partnerships with Federal and SLTT government entities. ASBDC found SBA online offerings are available in all 63 SBDC networks, and almost all networks provide links to SBA export assistance sites, though some SBDCs request clients to first seek counseling. Access to other federal agency resources varied and depended on the specialized needs of the SBDC program offerings.

The existing Federal Government cybersecurity resources found in Appendix E are readily available to small businesses. Currently, some of these resources are accessed by SBDCs, but there is no consistent pattern or plan for how the resources are shared on their websites. The survey of SBDC websites found that Federal Communications Commission (FCC), NIST, SBA, and DHS resources are mentioned inconsistently across the SBDC networks.

There is considerable diversity among SBDCs to match the needs of their communities. The small business interests of a community are influenced by the local industry, natural resources, geography, weather, and culture. Nevertheless, there are some common cybersecurity needs for all businesses regardless of size. These factors further emphasizes the importance of the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) to

align diverse small businesses and SBDCs with national cybersecurity programs and best practices.

IV. Analysis

4.1 Federal Programs Available to SBDCs

DHS identified a sample of cybersecurity programs, projects, and activities offered from across the Federal Interagency that can be useful to small businesses. Appendix E identified 46 different programs, projects, and activities varying from awareness training to a repository of best practices for cyber planning and information sharing programs. Most resources identified in Appendix E are available online, making them readily accessible with little to no cost. However, it is recognized that the sheer number of programs available presents a challenge, and most small businesses lack the time and expertise to determine which programs best apply to their specific needs.

In addition, the programs are operated by federal and non-federal organizations using separate websites, program offices, and engagement efforts. While accessing any one program may be straightforward, it could be challenging for small businesses to know about all the available resources, identify how to combine resources to meet their specific needs, and integrate programs to address a complete cybersecurity risk management lifecycle. These factors could create complexity for businesses and can undermine the efficient and effective dissemination of cybersecurity program information to the small business community.

4.2 SBDC and Small Business Findings

The results of the external and internal surveys show that small businesses and SBDC states and hosts are very concerned about cybersecurity risks to small businesses. Small businesses frequently identified viruses, malware, and ransomware infiltrating through their systems as issues of concern. Many SBDCs perceive cybersecurity advisement and training as important, and an even greater percentage of small businesses indicated they do not have adequate access to resources. Nonetheless, not all SBDCs are accessing federal resources and most small businesses are not aware of them. Small businesses most frequently identified training for managers and direct help with planning as important. However, they collectively identified the full range of resources as important, possibly indicating that small businesses need help identifying and prioritizing their cybersecurity needs.

The above findings indicate that small businesses need the type of service often provided by SBDCs. The results also show that SBDCs need the programs, projects, and activities often provided by the Federal Government. To provide small businesses with the most effective resources in the most efficient and cost-effective fashion, SBDCs would need information about Federal Government resources categorized and defined in terms of relevance to small businesses. In addition, SBDCs would need tools to help them quickly assess and evaluate which resources are best matched with the needs of small businesses.

According to the internal survey, 88 percent of the small businesses feel they are at risk of a cyberattack. Nonetheless, the majority of SBDCs indicated they are ill-prepared to deliver cybersecurity advisement/training. The second highest ranked need identified by SBDCs was for advisor training. Small businesses ranked one-on-one counseling the most beneficial form of

assistance for learning about and planning cybersecurity efforts. The juxtaposition of small business risks and SBDCs readiness indicates SBDCs will need advisor training to enable cybersecurity counseling capabilities to meet small business needs.

Small businesses identified webinars and online tools as the second and third most beneficial forms of assistance for learning about and planning cybersecurity efforts. More than 40 percent of business owners indicated a need for training seminars, webinars, and workshops. The third highest ranked need, as identified by SBDCs for developing cybersecurity programmatic readiness, was for client materials. 85 percent of SBDCs have not created workbooks or guides for small businesses primarily because they lack the requisite knowledge and expertise to development them. An analysis of small businesses need for training indicates an opportunity to address those needs with online client materials, many of which already exist and are available from the Federal Government, such as the DHS CISCP.

Federal cybersecurity programs are operated and maintained by a variety of organizations and agencies with different missions, and can be linked by the Cybersecurity Framework. Many program resources are frequently updated to match the rapidly changing cyber threat environment. Alignment with the Cybersecurity Framework can help small businesses efficiently and effectively access the most up-to-date resources, and participate in an interoperable cybersecurity programs which are aligned to best practices. SBDCs need to be able to access the most up-to-date version of resources and quickly share the information aligned with small business needs.

4.3 How SBDCs Leverage Government Partnerships and Use Federal Programs

The analysis shows some SBDCs are accessing federal programs to support the needs of their small business customers. Individual SBDC websites provide links to small business owners and operators with federal data from the Bureau of Labor Statistics, regulatory information from the Department of Labor and lending, disaster, and online learning courses from SBA. SBDC counselors serve as intermediaries, helping guide small businesses to the most appropriate federal resources to support their unique needs.

Opportunities exist to coordinate and expand upon current partnerships. Some SBDCs provide federal cybersecurity resources and tools (such as guidebooks and tip sheets) via their websites, but there are gaps and inconsistencies. A few include state and local resources, while others focus primarily on SBDC developed materials. Currently, several SBDC networks (16 of the 63 analyzed) provide cybersecurity training and counseling in various forms. These resources vary greatly in scope and content because they have developed organically rather than following a common or standardized approach.

Several challenges will need to be overcome before SBDCs can provide high-quality cyber support for small business concerns. SBDCs will need to understand the available cybersecurity resources and develop structured cyber consultation and referral capabilities tailored to the capabilities of their small business clients. The uniformity of cybersecurity needs across all organizations and lines of business will standardize pathways for developing SBDC expertise and cybersecurity services.

Federal partnerships offer a proven approach for assisting SBDCs to expand their service offerings. Current SBDC training on international trade serves as a model to build SBDC expertise in cybersecurity topics. Individual SBDC networks developed expertise in international

trade counseling to address a growing interest across their national body of organizations. To expand this specialized training expertise, SBDC advisers partner with and receive training from the SBA and the Department of Commerce (DoC) on the basics of international trade, international business and banking, and export and import regulation. More advanced private sector training is available for clients who wish to develop greater skills. In conjunction with SBDC export counseling, SBDCs also regularly host export regulation workshops provided by DoC. Training for these expert advisers is also regularly provided at the ASBDC annual conference. The framework used to expand international trade expertise throughout the SBDC network is being explored as a model for increasing cybersecurity programming where it does not currently exist.

Private sector partnerships can also be helpful to SBDCs. SBDCs have become proficient at providing training and support by working with private sector entities. For example, SBDCs have established a long-term partnership with Intuit to provide training and support for their small business accounting products. These training sessions are often customized for the business and their advanced accounting system needs. Support training for these private sector collaborations is regularly provided at the ASBDC annual conference.

The Michigan and Pennsylvania SBDCs offer working models that could be expanded and replicated across SBDCs. Michigan's Small Business Big Threat program builds on SBA, NIST, and private sector materials to offer a small business cybersecurity planning and assistance service. The Michigan SBDC has expanded its effort to involve at least four other SBDCs in Alabama, Missouri, Virginia, and West Virginia. The Pennsylvania SBDC provides a similar service using SBA, NIST, DHS, and FCC information. These offerings contain valuable cybersecurity support for SBDC clients; however, it is difficult for SBDCs to compile and maintain current and complete information from multiple sources on evolving cybersecurity risk management strategies.

V. Recommendations

Subject to available resources and approval, the following recommendations describe how SBDCs can leverage Federal Government programs, projects, and activities to improve access to high-quality cyber support for small business concerns:

- Centralize cybersecurity information and resources on the SBA website to be easily accessible by SBDC advisors and businesses;
- Provide a needs/risk-based resource mapping tool;
- Compile a digital directory of resources;
- Provide access to existing cyber training resources;
- Extend advisor expertise on cybersecurity across SBDCs through training;
- Expand the cyber advising expertise community of practice;
- Produce and provide access to information sharing training for SBDCs;
- Produce and provide access to guidebooks for small businesses;
- Develop promotional campaign and research cycle; and,

- Provide access to vetted and verified cyber solution on General Services Administration (GSA) schedule for volume-based discounts to SBDCs.

5.1 Plan to Increase SBDCs Access to Existing Federal Programs

The survey analysis indicates small businesses need SBDC services to provide them with individual plans, guidance, and assistance, and SBDCs need access to Federal Government programs, projects, and activities. The analysis of existing federal resources reveals the challenges small businesses and SBDCs may face when trying to identify which federal programs to leverage or apply.

To provide small businesses with the most useful resources in the most efficient and cost-effective fashion, SBDCs would need access to information on federal cybersecurity resources categorized and defined in terms relevant to small businesses. In addition, SBDCs would need tools to help them quickly assess and evaluate which resources are best matched with the needs of individual small businesses. The following focused recommendations should be considered:

5.1.1 Centralize Cybersecurity Information and Resources on the SBA Website to be Easily Accessible by SBDC Advisors and Businesses

To address challenges with identifying federal resources, DHS and SBA should collaborate to centralize information for SBDCs and small businesses. The goal is to provide an easy to navigate and use online interface, to help users quickly identify and access the most applicable federal programs, projects, and activities.

SBA should increase access for SBDCs to cybersecurity reference guides, videos, and other products on its SBA Partner Training Portal (The Portal). The Portal is designed to serve SBA resource partners, such as SBDCs, and other individuals who counsel and train small businesses. The expanded site would comprise SBA content and link to products and services offered by DHS and other federal organizations. To the greatest extent possible, products should be organized by program sophistication and aligned to the Cybersecurity Framework (see digital directory recommendation in Section 5.1.3).

5.1.2 Provide a Needs/Risk-based Resource Mapping Tool

To address challenges with identifying appropriate federal programs, DHS and SBA, in coordination with other federal departments and agencies, should collaboratively develop a tool to help identify the available resources to address different cybersecurity issues. One idea is a roadmap or information graphic designed to guide SBDC advisors and SMBs through the resource selection process based on the businesses' prioritized needs and level of cybersecurity sophistication. The Cybersecurity Framework Implementation Tiers[10] may provide the basis for this categorization. The information graphic can serve as a primary image on the SBA website (see recommendation in Section 5.1.1). SBDC advisors would be encouraged to use the roadmap in their day-to-day counseling with small businesses.

Over time, DHS can build an interactive tool that incorporates needs and risk-based assessments with the Cyber Security Evaluation Tool and the Cyber Resilience Review (CRR) assessment services and tools. The needs/risk-based tool would assess a holistic range of factors, including supply chain and which federal programs can produce the greatest value for the unique needs of

[10] https://csrc.nist.gov/csrc/media/publications/nistir/8170/draft/documents/nistir8170-draft.pdf

the small business. SBDCs would use the tool to produce engagements with small business with the greatest positive impact.

5.1.3 Compile a Digital Directory of Resources

SBDCs and small businesses should also be able to search all federal cybersecurity resources. DHS should start with the resources listed in Appendix E to conduct an analysis of available cybersecurity programs, projects, and activities, and develop a comprehensive digital cybersecurity resource directory. DHS should create meta-tag descriptions for each product and categorize the products by topic (e.g., cybersecurity threats, information sharing), type of product (e.g., guidance, tip sheet), and format (e.g., print material, video). The products can also be categorized by the Cybersecurity Framework Implementation Tiers or Core Functions. The directory would for the first time provide a logical construct for distinguishing the purpose and value of each cybersecurity product. The directory should serve as the main content of the SMB page on the Critical Infrastructure Cyber Community (C^3 - pronounced "C Cubed") Voluntary Program website.[11] SBDC counselors can use the directory as a stand-alone product to advance cybersecurity best practices and promote Federal Government cybersecurity resources.

5.2 Methods for Providing Counsel and Assistance to Improve a Small Business Concerns Cybersecurity Infrastructure, Awareness of Cyber Threat Indicators, and Cyber Training Programs for Employees

Survey analysis indicates SBDCs need advisor training to enable cybersecurity counseling capabilities and to meet small business needs. Training is also an opportunity to address those needs with online material, and direct SBDCs to free Federal Government resources. The following focused recommendations should be considered:

5.2.1 Provide Access to Existing Cyber Training Resources

To address the immediate need for materials, SBA and ASBDC should provide SBDCs with access to existing cyber training courses so that SBDCs can then deliver them to small business clients with varying technical capabilities. SBDCs are already using some Federal Government resources, and there is an opportunity to standardize those resources and make them more robust. Note that a legal review of the development agreements must be conducted to determine how federal course content can be used by private industry. The curriculum provided should address topics relevant to small businesses including network protection and defense, law enforcement post-breach, and intelligence on cyber threats.

Entry-level courses should help small businesses understand the nature of cyber threats and the potential vulnerabilities all businesses face. More advanced courses should be customizable to address the threats most relevant to different business models and provide instruction on how businesses can take explicit action to respond and recover from a cyber incident.

Cyber training courses should be provided both online and as basic training seminars or webinars. This allows rural businesses to access the curriculum and enable broader dissemination to the small business community. Courses should incorporate best practices learned by SBDCs currently providing similar cybersecurity training.

5.2.2 Extend SBDC Cyber Advisor Expertise through Cybersecurity Training

[11] https://www.dhs.gov/ccubedvp

To enable cybersecurity counseling capabilities, ASBDC should collaborate with SBDCs, SBA, and DHS to train SBDC advisors across the country on the skills necessary to guide and assist small businesses with cybersecurity planning. A series of train-the-trainer events, courses, or webinars should be used to help SBDCs understand how to use resource mapping tools and the directory of resources (Section 5.1). The program should be based on the Cybersecurity Framework Implementation Tiers to ensure programs are interoperable and aligned to best practices. ASBDC should leverage the existing programs developed by SBDCs as a starting point for any new "train-the-trainer" programs. Additional information on existing programs and cost-effective methods for implementation can be found in Appendix A and Appendix B.

Delivery of basic cybersecurity training should be based on the international trade training model provided by SBA and DoC (Section 4.3). Major SBDC networks should be encouraged to partner with and extend services into smaller networks. ASBDC and SBA can partner with federal departments and agencies and leverage existing federal materials to develop basic training modules.

The intent of the "train-the-trainer" courses is to provide SBDC advisors with a fundamental understanding of cybersecurity, and the expertise to advise small businesses on the range of resources available to small businesses. These courses should not be designed to turn SBDC advisors into high-level cybersecurity experts. SBDC advisors would guide their small business clients to select and apply tools and participate in programs to assess their cybersecurity posture, develop a plan for addressing vulnerabilities, and access the resources necessary to implement best practices.

5.2.3 Expand the Cyber Advising Expertise Community of Practice

ASBDC should continue to host an offline community of practice through workshops and conferences, and partner with SBA to develop an online engagement that connects SBDCs already involved in cybersecurity education efforts with SBDCs that are developing cybersecurity capabilities. Regular training opportunities should be provided at the annual national SBDC conference and regional and state SBDC meetings. These training opportunities combined with conference calls and webinars would provide frequent opportunities for SBDCs to share best practices (Appendix B).

A long-term goal could be providing SBDC advisors with opportunities to develop more advanced cybersecurity knowledge and skills. This would allow SBDCs to assist more sophisticated clients, including small businesses in high-tech sectors and organizations such as federal contractors that must adhere to stringent cybersecurity standards.

5.2.4 Produce and Provide Access to Information Sharing Training for SBDCs

A variety of information sharing programs provide awareness of actionable cyber threat indicators. These include independent information sharing and analysis organizations (ISAOs), Federal Government programs, and commercial service providers (Appendix C). However, direct participation in many information sharing programs would require investments and technical knowledge more than the resources available to most small businesses.

SBA and DHS, with input from ASBDC, should produce and provide access to both in-person and online training for SBDCs. These courses would educate SBDCs on information sharing and information sharing programs, as well as the requirements and strategies for participation.

5.2.5 Produce and Provide Access to Guidebooks for Small Businesses

DHS should lead the development of a series of guidebooks and tip sheets. These should build off the informational efforts already developed by SBDCs such as the New York SBDC's Cyber Security Planning Guide. Along with training, SBDCs can use these guidebooks to counsel small businesses on which information sharing programs are less resource intensive and align to the organization's needs and capabilities. SBDCs can also provide introductions and help small businesses fill out applications. When information sharing programs are not accessible to small businesses, they can often join an association or pay a commercial service provider to participate directly in the program on behalf of its stakeholders. SBDCs can provide referrals and counsel small businesses on ways to participate indirectly through these associations. ASBDC should also produce tip sheets and other materials that SBDCs can distribute to small businesses when providing consultation and referral services.

5.2.6 Develop a Promotional Campaign and Research Cycle

DHS should develop a communications campaign to promote DHS and SBA cybersecurity resources. The campaign would encourage SBDCs to use cybersecurity products, services, and educational events, and increase traffic to the C^3 Voluntary Program website and SBA portal. Campaign activities may include conducting virtual roundtables with SBDC advisors; creating website and product promotions for SBDCs; and incorporating website promotions in SBDC training programs. Other elements could include: establishing relationships with professional associations serving SMBs; working with DHS Cyber Security Advisors (CSAs) to strengthen SBDC relationships through office visits and event participation; and using social media to engage small businesses and promote available cybersecurity resources.

Continued research is essential to inform recommendations implementation and to track changes in the evolving landscape of small businesses and federal programs. SBA should conduct expanded and periodic surveys of SBDC and small business needs, and then work with DHS to further define and update requirements. DHS should work with government and private sector organizations to identify and incorporate new programs, projects, and activities. DHS and SBA should periodically review identified resources and requirements to more efficiently allocate investments, close gaps, and coordinate federal activities.

VI. Conclusion

Small businesses are fully cognizant that they need to take additional measures to protect against potential cyber threats. DHS and SBA recognize the opportunity to strengthen small business cybersecurity by working with the SBDCs. This strategy shares information on what SBDCs need to consistently connect their small business clients to federal cybersecurity programs, projects, and activities. Together DHS, SBA, and SBDCs will strengthen small businesses' cyber defense by overcoming the common cybersecurity challenges of information sharing and access to government resources, and by making it easier for small businesses to address the full cybersecurity risk management lifecycle.

Appendix A: Education and Awareness Training

Recommendation 5.2.2 suggests that a SBDC leverage the existing education and training as a starting point for developing new "train-the-trainer" programs. Additional information on existing programs can be found below in this appendix. Where possible, the education and training resources are listed with available summaries and descriptions.

The SBDC network provides access to cybersecurity awareness and training to small business concerns. In-person training is offered through workshops and consultations hosted by SBDC advisors and their trusted partners. Virtual training is provided through webinars, remote classrooms, and customized cybersecurity education portals. SBDCs often enlist the assistance of technology partners and other cybersecurity experts, including federal representatives, during SBDC training sessions.

SBDCs' linkage with federal resources such as the DHS C^3 Voluntary Program, NIST, the Federal Bureau of Investigation, the Federal Trade Commission (FTC), the National Initiative for Cybersecurity Education and others identified in Appendix E have increased host organization, mentor, and client awareness of these federal services in their communities.

Online Portals Serving the SBDC Network

SBDC Online Learning Center

While SBDCs offer a wide range of virtual resources to their clients, many chose to leverage centralized tools such as the Global Classroom (supported by Microsoft). This resource allows individual SBDCs to customize instructional offerings to share with their small business clients.

Learn more at www.globalclassroomnetwork.com/.

SBA Partner Training Portal

SBA's Partner Training Portal is designed to offer Agency Resource Partners such as SBDC, SCORE, and Women's Business Centers, direct access to online training material related to federal resources of interest to their clients. The platform features programmatic and policy overviews for finance, procurement, disaster recovery, and other SBA offerings so mentors have immediate access to the latest information.

Learn more at https://www.sba.gov/ptp.

Examples of SBDC Cybersecurity Education Programs

Kansas SBDC
Cybersecurity Center for Small Business

The program, opened in October 2017, has four major components:

1. Comprehensive online assessment that addresses a company's cybersecurity risk including Health Insurance Portability and Accountability Act and NIST 800-171 compliance;
2. Live (both in-person and online) and asynchronous education on cybersecurity and general concepts, as well as business policy and procedures;
3. Technical assistance referrals; and,

4. Client prioritization and tracking.

The center provides most of its services through a virtual platform. Once in the system as a Cybersecurity Center for Small Business client, users of the virtual platform will have access to training and information created by partnerships made this year. The training platform will take training programs developed by partners like the National Cyber Security Alliance (NCSA), the FTC, and other America's SBDC networks and synthesize them for Kansas business.

Michigan SBDC

Small Business Big Threat

The Michigan SBDC team has built a robust cybersecurity education portal called Small Business, Big Threat to provide assessments, in-depth training, resources, and Spanish language tools.

Learn more at https://smallbusinessbigthreat.com/.

New York SBDC

The New York SBDC cybersecurity resource offers newsletters, tips, and a downloadable Cybersecurity Planning Guide.

Learn more at http://www.nyssbdc.org/resources/cybersecurity.html.

Georgia SBDC

CyberStrength

Georgia's SBDC cybersecurity platform provides an events calendar, articles, tips, and a customized program offering called CyberStrength. CyberStrength is an initiative to provide an incentive-based approach to building a cybersecurity plan versus a defensive-based reaction to malware, a hack, ransomware, or other cyberattack.

Delaware SBDC

DatAssured

The DatAssured program resource raises awareness of cyber risk within Delaware's small business community, helps businesses manage the threat and impact of cyber interference, and fosters innovation in cybersecurity by providing direct outreach and support to Delaware's small businesses. It also provides workshops, events, a risk assessment tool, online training, tips, templates, and a workbook for download.

Learn more, visit delawaresbdc.org/special-programs/datassured/

The Delaware SBDC's Small Business Cybersecurity Workbook provides small business with a starting concept for creating a written information security program.

Learn more at http://delawaresbdc.org/wp-content/uploads/2016/09/Delaware-Small-Biz-Cybersecurity-Workbook.pdf.

Oregon SBDC

Small Business Cyber Center

Oregon's Small Business Cyber Center is a specialized program to provide cybersecurity advising, training, and resources. Mt. Hood Community College leads the SBDC's efforts to work closely with the business community, government agencies, and law enforcement to combat cyber criminals through a proactive awareness plan.

Learn more at http://cyberoregon.com/.

SW Texas Border Region SBDC (San Antonio)

Center for Infrastructure Assurance and Security

The Center for Infrastructure Assurance and Security is developing the world's foremost center for multidisciplinary education and development of operational capabilities in the areas of infrastructure assurance and security. The University of Texas at San Antonio is part of the Center for Infrastructure Assurance and Security. The SW Texas SBDC also works with the Procurement Technical Assistance Center to promote cybersecurity for government contractors.

Learn more at http://cias.utsa.edu/ and https://ptac.txsbdc.org/cybersecurity-for-small-business/.

Idaho SBDC

Idaho SBDC's website includes an assessment tool, training courses, and links to important information for clients to identify risk, protect businesses, detect intrusions, and recover from an attack.

Learn more at http://idahosbdc.org/cyber.

Other SBDCs

There are many SBDCs offering cybersecurity programs or resources, directly or through referral, to their clients. Those SBDCs frequently reference federal resources on their web portals, print materials, or during classroom trainings. Ongoing access, understanding, and local knowledge of area resources could be enhanced for those SBDCs that do not currently offer cybersecurity education services.

Additional Non-Federal Resources

The Federal Government does not endorse specific corporations, however, the following organizations and products are included for your information and convenience. This is not intended to be a comprehensive list.

Center for Internet Security
Center for Internet Security (CIS) is a forward-thinking, non-profit entity that harnesses the power of the global IT community to safeguard private and public organizations against cyber threats. CIS Controls and CIS Benchmarks are the global standard and recognized best practices for securing IT systems and data against the most pervasive attacks. These proven guidelines are continuously refined and verified by a volunteer, global community of experienced IT professionals. CIS is home to the Multi-State Information Sharing and Analysis Center®, the go-to resource for cyber threat prevention, protection, response, and recovery for U.S. SLTT government entities.

Learn more at www.cisecruity.org.

Geographically-Specific Resources
State and local government offer geographically specific cybersecurity resources. This collection of cyber resources from various levels of government can help SMBs recognize and address their cyber risks.

Learn more at https://www.us-cert.gov/ccubedvp/sltt#geo.

National Conference of State Legislatures Security Breach Notification Laws
48 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information. This site provides state by state requirements of data breach statutes.

Learn more at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

National Cyber Security Alliance
The NCSA builds strong public/private partnerships to create and implement broad-reaching education and awareness efforts to empower users at home, work, and school with the information they need to keep themselves, their organizations, their systems, and their sensitive information safe and secure online, and to encourage a culture of cybersecurity.

Learn more at https://staysafeonline.org/.

- *Online Holiday Shopping*
    - Prepared by the NCSA, this is a tip sheet for SMBs regarding the Holiday Shopping season.
    - https://staysafeonline.org/business-safe-online/resources/holiday-shopping-backgrounder

- *Technology Checklist of Businesses*
    - This tip sheet prepared by the NCSA is designed to help identify the technology in a business that needs to be protected.
    - https://staysafeonline.org/business-safe-online/resources/technology-checklist-for-businesses
- *Privacy is Good for Business 2017*
    - This infographic was prepared by the NCSA for SMBs regarding how to handle and protect personal information.
    - https://staysafeonline.org/business-safe-online/resources/privacy-is-good-for-business-2017
- *Creating a Culture of Cybersecurity*
    - This infographic is designed for SMBs and covers cybersecurity best practices in the work place.
    - https://staysafeonline.org/business-safe-online/resources/creating-a-culture-of-cybersecurity-from-the-break-room-to-the-boardroom-infographic
- *Creating a Culture of Cybersecurity in your Business*
    - Prepared by the NCSA, this infographic provides information on cybersecurity best practices.
    - https://staysafeonline.org/business-safe-online/resources/creating-a-culture-of-cybersecurity-in-your-business-infographic

Small Firms Cybersecurity Guidance: How Small Firms Can Better Protect Their Business
The Securities Industry and Financial Markets Association created this page to provide information applicable to small firms, supporting their overall business model to increase security and ensure customer protection.

Learn more at http://www.sifma.org/issues/operations-and-technology/cybersecurity/guidance-for-small-firms/.

The Current and Future Landscape of Identity Theft: Findings of the "Identity Theft and Nexus to Illicit Activity" Team
This is a paper discussing Identity Theft (IDT) and its growing risk to SMBs.

Learn more at https://www.rti.org/sites/default/files/resources/idt-whitepaper-final-20131030.pdf.

Countering IDT Through Education and Technology
A 2014 Identity Theft and Nexus to Illicit Activity Team comprised of public and private sector analysts created an infographic with some protective measures to address IDT incidents of individuals and organizations. The infographic can be used to guide decision making and learn steps to mitigate identity theft.

The infographic is available at
https://www.rti.org/sites/default/files/resources/xpl_bmgf_1404_idtphase2_r02.pdf.

The Changing Face of IDT: The Current and Future Landscape
This is an infographic covering IDT and its growing risk to SMBs.

Learn more at
https://www.rti.org/sites/default/files/resources/xpl_bmgf_1302_id_theft_brochure_r03_pages.pdf.

Appendix B: Ways to Expand the Cyber Advising Expertise Community of Practice

The SBDC network accesses and shares operational, programmatic, and best practice information. Existing programs, events, and platforms provide the opportunity to distribute materials and best practices throughout the network.

The following recommendations maximize existing outlets to increase cybersecurity education for the SBDC network in a cost-effective manner.

A. Both SBA's SBDC Advisory Committee and ASBDC's Board of Directors could benefit from periodic briefings on cybersecurity education, trends, and resources. Briefings could be offered by federal officials, industry professionals, and talented practitioners. SBA and ASBDC may also wish to solicit cybersecurity professionals for appointment to either advisory body.

B. The ASBDC manages an annual conference that draws a large group of network mentors each year. While SBA and ASBDC have previously partnered on tracks focused on specialized export assistance, and the conference currently includes existing cybersecurity workshops, an assessment of a dedicated track on this topic may be warranted for future conferences. Such a specialized track could also be connected to any cybersecurity certifications of interest to SBDC advisors. Similarly, regional conferences presented by SBDC host institutions may provide settings for dedicated cybersecurity education campaigns.

C. Online platforms outlined in Appendix A, including the SBDC Online Learning Center and the SBA Partner Training Portal, could benefit from additional cybersecurity education materials. Content could be provided from existing sources including federal entities and SBDCs. Online platforms could be extended through the dedicated use of webinars featuring cybersecurity program specialists and experts who provide professional knowledge sharing with SBDC advisors. Sharing of threats alerts through federal communication channels could also be highlighted on existing platforms to maximize exposure.

D. The cybersecurity resource sample provided in Appendix E could be distributed, updated, and accessed in multiple formats by vested parties and SBDC advisors on a regular basis.

E. ASBDC could consider an annual assessment of SBDC advisor and host institution needs, interests, and feedback concerning available cybersecurity resources to promote customer-centric improvements shared with federal program officials.

Appendix C: Guidance on Entering Agreements with Information Sharing and Analysis Organizations

Introduction to Information Sharing and Analysis Organizations[12]

The importance of information sharing to data security has been discussed for well over a decade. Early realization of its importance led to the creation of Information Sharing and Analysis Centers (ISACs) for critical U.S. infrastructures to ensure the protection of information systems and the physical assets supporting them. While this was an important step toward establishing a system for sharing information related to cybersecurity, most government and industry organizations are not part of a critical infrastructure. In February 2015, the White House issued Executive Order (EO) 13691, *Promoting Private Sector Cybersecurity Information Sharing*, which called for the Secretary of DHS to "strongly encourage the development and formation of ISAOs." This EO acknowledged broader information sharing (beyond critical infrastructures) was needed to better protect the Nation from cyber incidents. These new entities could be "organized on the basis of sector, subsector, region, or any other affinity," greatly expanding the number and type of potential information sharing organizations developed to meet the goal of a more comprehensive information sharing environment. In turn ISACs are an example of a type of ISAO.

To help with the establishment of ISAOs, EO 13691 directed DHS to "enter into an agreement with a non-governmental organization to serve as the ISAO Standards Organization." The ISAO Standards Organization, in turn, established working groups made up of leading information security community professionals to address specific areas pertinent to creating or operating ISAOs. When developing the various documents, the working groups considered the two primary functions important to ISAOs: the sharing of cybersecurity information and the analysis of the shared information. The purpose of these efforts is ultimately to improve the ability of organizations to, as outlined in the EO, "detect, investigate, prevent, and respond to cyber threats" while protecting the privacy and civil liberties of citizens.

Diverse communities of interest require a flexible and scalable framework tailored to meet the unique needs of each constituent group while remaining grounded in a shared set of principles. Accordingly, ISAOs will vary in terms of size, objectives, and capabilities. Both commercial and not-for-profit entities have been (and will be) formed to provide services to ISAOs or to become ISAOs themselves. Some ISAOs may be created informally and may have little or no desire to collect and analyze information in near-real-time for their members. Other ISAOs may be highly interested in near-real-time analysis and dissemination of actionable information to better protect their members, and may have a goal to help respond to security incidents affecting their members. Which type of ISAO is formed and what services it offers will be decided by its members to address their needs and their cyber risk management objectives. Specific capabilities may also be required before sharing cybersecurity information with certain government agencies or industry organizations. While not part of the reason for sharing information, establishing ISAOs may have the additional benefit of spurring innovation and the creation of new services and techniques to assist in the goal of securing the nation and, especially, the digital economy.

[12] https://www.isao.org/wp-content/uploads/2016/10/ISAO-100-1-Introduction-to-ISAO-v1-01_Final.pdf

What is an ISAO?[13]

A common and natural question continually arising is, "What is an ISAO?" There have been various definitions published with slight variations among them. The primary characteristic of an ISAO in the cybersecurity information sharing ecosystem is that the ISAO analyzes and shares information related to cybersecurity risks and incidents between and among its membership. This holds true across a wide range of ISAOs with varying constituent membership organizations, regardless of whether they are affiliated with a critical infrastructure. The definition referenced by ISAO 100-1 Introduction to ISAOs is found in 6 U.S.C. §131(5) and reads as follows:

"The term Information Sharing and Analysis Organization means any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of—

A. Gathering and analyzing critical infrastructure information, including information related to cybersecurity risks and incidents, in order to better understand security problems and interdependencies related to critical infrastructure, including cybersecurity risks and incidents and protected systems, to ensure the availability, integrity, and reliability thereof;
B. Communicating or disclosing critical infrastructure information, including cybersecurity risks and incidents, to help prevent, detect, mitigate, or recover from the effects of an interference, compromise, or incapacitation problem related to critical infrastructure, including cybersecurity risks and incidents, or protected systems; and
C. Voluntarily disseminating critical infrastructure information, including cybersecurity risks and incidents, to its members; state, local, and federal governments; or any other entities that may assist in carrying out the purposes specified in subparagraphs (A) and (B)."

Despite the statute's language on critical infrastructure information, ISAOs are important to the cybersecurity information sharing ecosystem, because they enable the analysis and sharing of information related to cybersecurity risks and incidents between and among members or customers, which may or may not be affiliated with a critical infrastructure. It is clear from reading EO 13691 that there is a recognition that ISAOs will be formed in sectors and communities not directly tied to any critical infrastructure. For the ecosystem to flourish, it will include ISAOs that may not exchange information with a critical infrastructure.

Value Proposition of ISAOs

Fundamental to the establishment of an ISAO is the value proposition offered to its participants, members, and collaborators. An ISAO must provide a tangible benefit for it to attract and enroll members. ISAOs offer benefits to their members and other ISAOs, including the following:

- Provide an informative set of cybersecurity threat information and operational practices to help individual members be more secure;
- Establish and maintain trusted relations among members by establishing a framework of common, shared values and expectations;
- Enhance members' situational awareness and knowledge about how to protect themselves from, detect, and react to cyberattacks;

[13] https://www.isao.org/wp-content/uploads/2016/10/ISAO-100-1-Introduction-to-ISAO-v1-01_Final.pdf

- Aggregate information from multiple organizations. ISAOs can present a richer picture of malicious activity taking place within a specific sector, geographic region, the nation, or the world. Member organizations can use this enriched information to improve their individual and collective security, blocking attacks they would not have seen otherwise;
- Exchange information between members to help them carry out effective and timely responses when they discover cybersecurity incidents, attacks, or unauthorized intrusions;
- Share non-incident information such as best practices, training opportunities, processes and procedures, and product information to enhance a member's security program; and
- Contribute to lower costs and barriers of entry for cybersecurity information sharing.

Sharing of Information

There are many issues to be addressed when an ISAO considers its involvement in the actual sharing of information—and as always, this will be decided by its members and their objectives. For example, what information will the members be asked to share? How will the sharing of information be accomplished? How will privacy be maintained? What level of trust can the members place in the information? Will the ISAO receive information from other non-member entities (such as the government or other ISAOs), and if so, will this be a one-way sharing of information or will it be bi-directional? ISAOs will exist in the ecosystem in every combination of sharing as discussed here. These issues are at the heart of any information sharing program. An emerging ISAO does not need to face these issues in isolation, however, as there are individuals and organizations (such as the ISAO SO) to help them address these questions systematically.

ISAO Membership Fees

Whether or not an ISAO charges its members a fee will depend on the goal of the ISAO and the services it offers. Many things can be done to share information without requiring a full-time ISAO staff or a membership fee. There are other services and capabilities requiring full-time personnel to accomplish, which may drive consideration of a fee-based business model. Some ISAOs may have a mix of paid memberships and unpaid memberships to offer a combination of free and premium services.

Analysis of Information

Up to this point, the emphasis has been on the sharing of information. An important function of an ISAO is the dissemination of actionable information, which requires analysis. The extent of the analysis needed will depend on the goal of the ISAO and its members. A well-tailored analytical capability will make the difference between inundating members with data that provides no help, and disseminating information that can help members take actions to enhance their security posture.

Information Security

ISAOs will vary in size, sophistication, and abilities. They will also vary in the amounts and types of information they share. However, all ISAOs, no matter how established or new, face common security challenges. ISAOs need to consider these security challenges and include security considerations at the beginning of the ISAO's business process through appropriate governance, risk, and security policies. Determining security protocols can facilitate success, as

ISAOs and their members will be more effective in building trust among the members, and between the members and the ISAO. Established ISAOs may also use this guidance to assess their own security. Addressing security as part of overall ISAO governance enables ISAO members and prospective members to make appropriate risk decisions about their participation in information sharing activities.

Security policies of an ISAO may vary to reflect the various types of information being shared, the different degree of sensitivity of that information, and how information is shared amongst and between members. For example, a security policy related to sharing automated indicators likely will be different from a security policy related to sharing PDF documents. Similarly, the policy for storing open source news might differ from the policy for storing sensitive and otherwise confidential or non-public member submissions.

An ISAO's membership may also drive the levels of security needed. ISAOs whose members individually have robust security capabilities will likely have more robust security procedures together as an ISAO, than ISAOs whose members have less advanced capabilities. Differences in an ISAO's and members' general capabilities may be driven by disparate legal requirements, risk tolerance, industry practice, or maturity in the information sharing ecosystem. Regardless of whether an organization is for-profit or non-profit, large or small, security is an important component of an ISAO's success.

The 2015 *Cyber Information Sharing Act* required guidance[14] issued by the Department of Justice (DoJ) and DHS outlines procedures for private sector entities to follow when sharing cybersecurity information with the Federal Government. The guidance also includes basic structures and security requirements companies must meet to participate in the information sharing process with DHS. In addition to covering how to identify and share cyber threat indicators and defensive measures, the joint DoJ-DHS Guidance explains how to share that information with federal entities through the Federal Government's capability and process that is operated by DHS. The *Cyber Information Sharing Act* outlines ways non-federal entities can share cyber threat indicators and defensive measures through the DHS capability and process created under section 105(c) of the Act. Non-federal entities sharing cyber threat indicators and defense measures via the AIS initiative, web form, email, or other government information sharing programs are eligible for liability protection. Although ISACs and Information Sharing and Analysis Organizations are usually private entities, Section 106(b)(1) of the *Cyber Information Sharing Act* notes that sharing threat indicators and defensive measures via one of those channels also receives liability protection.

Furthermore, the joint DoJ-DHS Guidance explains how to share such information with DHS and other federal entities—including law enforcement—through other means authorized by the *Cyber Information Sharing Act*, and discusses the various legal protections the Act provides for such authorized sharing.

---

[14] In February 2016, DHS and the DoJ jointly issued the *Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government* in accordance with the *Cyber Information Sharing Act*. The guidance requires federal entities to establish and maintain procedures and implement protocols that facilitate and promote the sharing of cybersecurity information by the Federal Government in a timely manner. It encourages the Federal Government to share classified and unclassified cyber threat indicators and defensive measures with both Federal and private entities as broadly and as quickly as possible. In addition, the guidance describes mechanisms through which the appropriate federal entities can share information with the private sector.

CISA also defines strong privacy protections, which are further detailed in companion documents. Not all ISAOs will participate in this DHS program, for a variety of reasons, but DHS guidelines may serve as an important reference for ISAOs choosing to participate in the program. ISAOs who choose not to participate might still benefit from an understanding of the security requirements of CISA and the AIS program at least as a comparison, as they develop and implement their own information sharing policies and procedures. DHS and DoJ have issued CISA implementation guidance for the private sector.

Learn more at https://www.isao.org/.

Additional Information Sharing Programs

Automated Indicator Sharing[15]

DHS's free AIS capability enables the exchange of cyber threat indicators between the Federal Government and the private sector. Threat indicators are pieces of information such as malicious IP addresses, the sender address of a phishing email, or much more complicated information.

AIS is a part of the Department's effort to create an ecosystem where as soon as a company or federal agency observes an attempted compromise, the indicator will be shared in real time with Department partners, protecting them from that threat. Real-time information sharing means adversaries can only use an attack once, which increases their costs and ultimately reduces the prevalence of cyberattacks. While AIS will not eliminate sophisticated cyber threats, it will allow companies and federal agencies to concentrate more on them by clearing away less sophisticated attacks.

Ultimately, the goal is to commoditize cyber threat indicators through AIS, so that tactical indicators are shared broadly among the public and private sector, enabling everyone to be better protected against cyberattacks.

Learn more at https://www.dhs.gov/ais.

Cyber Information Sharing and Collaboration Program[16]

Information sharing is a key pillar of effective cybersecurity. By sharing information rapidly between the government and the private sector, network defenders can block cyber threats before damaging compromises occur. DHS'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

[15] https://www.us-cert.gov/ais
[16] https://www.dhs.gov/ciscp

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.

Learn more at https://www.dhs.gov/ciscp.

Enhanced Cyber Security Service[17]

DHS's Enhanced Cybersecurity Services (ECS) program is an intrusion prevention capability that helps U.S.-based companies protect their computer systems against unauthorized access, exploitation, and data exfiltration. ECS works by sharing sensitive and classified cyber threat information with accredited Commercial Service Providers. These providers can use the information to block certain types of malicious traffic from entering customer networks. ECS is meant to augment, but not replace, existing cybersecurity capabilities.

The ECS program currently offers three service offerings:

- Domain Name Service Sinkholing, which blocks access to specified malicious domain names;
- Email Filtering, which blocks email with specified malicious criteria from entering a network; and,
- Netflow Analysis, which uses passive detection to identify threats.

The ECS program continues to consider additional services that can use government-vetted cyber threat indicators to enhance the protection of U.S.-based organizations. There are three Communications Service Providers accredited to provide enhanced cybersecurity services:

- AT&T;
- CenturyLink; and
- Verizon

Learn more at https://www.dhs.gov/enhanced-cybersecurity-services.

[17] https://www.dhs.gov/enhanced-cybersecurity-services

Appendix D: Reference Guide on Referrals to Cyber-Area Specialists

Critical Infrastructure Cyber Community Voluntary Program[18]

DHS C^3 Voluntary Program is a focal point for cybersecurity outreach, education, and information for the Nation's 16 sectors of critical infrastructure. The C^3 Voluntary Program also serves SMBs, as well as departments and agencies at all levels of government.

Established by EO 13636, the program promotes use of the Cybersecurity Framework. The Cybersecurity Framework provides a flexible approach for identifying, assessing, and managing cyber risk. The approach is applicable to organizations of all sizes and all sectors.

The C^3 Voluntary Program also promotes DHS cybersecurity tools, best practices, and services. Some of these resources support sophisticated cybersecurity programs; others are appropriate for start-up programs.

DHS cybersecurity resources include technical assistance; voluntary assessments; sector-specific implementation guidance; cybersecurity toolkits for businesses and government agencies; and a suite of tools for conducting risk assessments, enhancing information sharing, and developing training and workforce development programs.

The C^3 Voluntary Program leads a range of educational efforts:

- Conducts webinars and forums on cybersecurity processes and practices;
- Delivers presentations to industry partners and professional associations;
- Collaborates with government agencies, sector coordinating councils, and organizations serving SMBs to advance best practices;
- Assesses and responds to information needs defined by the Nation's 16 critical infrastructure sectors;
- Manages the Department's central website for cybersecurity tools and resources for critical infrastructure; and
- Distributes a monthly bulletin featuring new resources and upcoming events.

For information, please visit https://www.us-cert.gov/ccubedvp or email ccubedvp@hq.dhs.gov.

National Cybersecurity and Communications Integration Center

DHS created the United States Computer Emergency Readiness Team (US-CERT)[19] in September 2003 to protect the Nation's internet infrastructure by coordinating defense against and response to cyberattacks. US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) [20] was later created to focus on coordinating efforts among Federal, SLTT, and control

[18] https://www.us-cert.gov/sites/default/files/c3vp/smb/CCubedVP_Outreach_and_Messaging_Kit_SMB.pdf
[19] https://www.us-cert.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf
[20] https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_ICS-CERT_S508C.pdf

systems owners, operators, and vendors to respond to and share information about control systems-related security incidents and mitigation measures.

In 2009, DHS created the NCCIC to bring together US-CERT, ICS-CERT and the National Communications Center operational elements under one organization. Throughout 2017, NCCIC realigned its organizational structure and integrated like functions previously performed independently by the US-CERT and ICS-CERT. This structure combines intersecting roles from the below legacy organizations to enhance the effectiveness of NCCIC's cybersecurity and communications mission.

NCCIC collaborates with federal departments and agencies, the private sector, the research community, SLTT governments, and international entities. By analyzing incidents reported by these entities and coordinating with national security incident response centers responding to incidents on both classified and unclassified systems, NCCIC disseminates reasoned and actionable cybersecurity information to the public.

NCCIC shares timely, actionable information to the broadest extent possible. Subscriptions are available to all users for:

- Weekly Vulnerability Bulletins – containing a summary of new vulnerabilities documented in the U.S. National Vulnerability Database the week prior, as well as patch information when available.
- Technical Alerts – providing users with information about vulnerabilities, incidents, and trends that pose a significant risk, as well as mitigations to minimize loss of information and disruption of services.
- Current Activity entries – containing a concise description of an issue and associated actions that a user can take to diminish exposure.
- Tips – detailing issues with broad appeal to NCCIC's constituents.

NCCIC is a key component of DHS's Strategy for Securing Control Systems. The primary goal of the strategy is to build a long-term common vision where effective risk management of control systems security can be realized through successful coordination efforts. NCCIC leads this effort by:

- Responding to and analyzing control systems-related incidents;
- Conducting vulnerability, malware, and digital media analysis;
- Providing onsite incident response services;
- Providing situational awareness in the form of actionable intelligence;
- Coordinating the responsible disclosure of vulnerabilities and associated mitigations; and,
- Sharing and coordinating vulnerability information and threat analysis through information products and alerts.

Strategy implementation creates a common vision with respect to participation, information sharing, coalition building, and leadership activities. Its implementation also improves coordination among relevant industrial control systems stakeholders within government and private industry, thereby reducing cybersecurity risks to all critical infrastructure sectors.

The NCCIC's Hunt and Incident Response Team (HIRT) provides onsite incident response, free of charge, to organizations that require immediate investigation and resolution of cyberattacks. In 2016, the incident response capabilities of US-CERT and ICS-CERT were combined to create HIRT, which operates under NCCIC and provides DHS's front line response for cyber incidents and proactively hunts for malicious cyber activity. Upon notification of a cyber incident, HIRT will perform a preliminary diagnosis to determine the extent of the compromise. At the customer's request, HIRT can deploy a team to meet with the affected organization to review network topology, identify infected systems, image drives for analysis, and collect other data as needed to perform thorough follow-on analysis. HIRT is able to provide mitigation strategies and assist asset owners/operators in restoring service and provide recommendations for improving overall network and control systems security.

Learn more at https://www.us-cert.gov/.

Cyber Resilience Review[21]

The Cyber Security Evaluation program, within DHS's NPPD, conducts a no-cost, voluntary, non-technical assessment to evaluate operational resilience and cybersecurity capabilities within critical infrastructure sectors, as well as SLTT governments through its CRR process.

The goal of the CRR is to develop an understanding of an organization's operational resilience and ability to manage cyber risk to its critical services during normal operations and times of operational stress and crisis. The CRR is based on the CERT Resilience Management Model, a process improvement model developed by Carnegie Mellon University's Software Engineering Institute for managing operational resilience. One of the foundational principles of the CRR is the idea that an organization deploys its assets (people, information, technology, and facilities) in support of specific operational missions (i.e., critical services). Applying this principle, the CRR seeks to understand an organization's capacities and capabilities in performing, planning, managing, measuring, and defining cybersecurity practices and behaviors in the following nine domains:

- Asset Management;
- Controls Management;
- Configuration and Change Management;
- Incident Management;
- Service Continuity Management;
- Risk Management;
- External Dependency Management;
- Training and Awareness; and
- Situational Awareness.

The CRR seeks participation from a cross-functional team consisting of representatives from business, operations, security, information technology, and maintenance areas within an organization. These representatives may include personnel with the following roles and responsibilities within the organization:

[21] https://www.us-cert.gov/sites/default/files/c3vp/crr-fact-sheet.pdf

- IT policy & procedures (e.g., Chief Information Security Officer);
- IT security planning & management (e.g., Director of Information Technology);
- IT infrastructure (e.g., network/system administrator);
- IT operations (e.g., configuration/change manager);
- Business operations (e.g., operations manager);
- Business continuity & disaster recovery planning (e.g., BC/DR manager); and
- Risk analysis (e.g., enterprise/operations risk manager).

Learn more at https://www.us-cert.gov/ccubedvp/assessments.

Cyber Security Advisors[22,23]

CSAs are regionally located DHS personnel who direct coordination, outreach, and regional support to protect cyber components essential to the sustainability, preparedness, and protection of U.S. critical infrastructure and SLTT governments. CSAs offer immediate and sustained assistance to prepare and protect SLTT and private entities. They bolster the cybersecurity preparedness, risk mitigation, and incident response capabilities of these entities and bring them into closer coordination with the Federal Government. CSAs represent a front-line approach and promote resilience of key cyber infrastructures throughout the United States and its territories.

The CSA program's primary goal is to assist in the protection of cyber components essential to the Nation's critical infrastructure. Equally important is their role in supporting cybersecurity risk management efforts at the state and local homeland security initiative levels. CSAs will work with established programs in State and local areas, such as Protective Security Advisors (PSAs), Federal Emergency Management Agency (FEMA) emergency management personnel, and fusion center personnel.

Protective Security Advisor Program[24]

In addition to the Cyber Security Advisor Program, NPPD operates the PSA Program. PSAs are security subject matter experts who engage with SLTT government mission partners and members of the private sector stakeholder community to protect the Nation's critical infrastructure. The PSA program maintains a robust operational field capability, with regional staff and PSAs serving in 73 districts in 50 States and Puerto Rico. The NPPD regional staff serve as the link to DHS infrastructure protection resources; coordinate vulnerability assessments, training, and other DHS products and services; provide a vital link for information sharing in steady-state and incident response; and assist facility owners and operators with obtaining security clearances.

The PSA program's primary mission is to proactively engage with federal and SLTT government mission partners and members of the private sector stakeholder community to protect critical infrastructure. Regional Directors oversee and manage the Department's PSA program in their respective regions, while PSAs facilitate local field activities in coordination with other DHS offices. The PSAs have five mission areas that directly support the protection of critical infrastructure:

---

[22] https://www.isao.org/resource-library/government-programs/dhs-cyber-security-advisors-csas/

[23] https://www.dhs.gov/xlibrary/assets/pso_cat_csc.pdf

[24] https://www.dhs.gov/sites/default/files/publications/PSA-Program-Fact-Sheet-05-15-508.pdf

- Plan, coordinate, and conduct security surveys and assessments – PSAs conduct voluntary, non-regulatory security surveys and assessments on critical infrastructure assets and facilities within their respective regions.
- Plan and conduct outreach activities – PSAs conduct outreach activities with critical infrastructure owners and operators, community groups, and faith-based organizations in support of the Office of Infrastructure Protection's (IP) priorities.
- Support National Special Security Events (NSSEs) and Special Event Activity Rating (SEAR) events – PSAs support federal, state, and local officials responsible for planning, leading, and coordinating NSSE and SEAR events.
- Respond to incidents – PSAs plan for and, when directed, deploy to Unified Area Command Groups, Joint Operations Centers, FEMA Regional Response Coordination Centers, and/or state and local Emergency Operations Centers in response to natural or man-made incidents.
- Coordinate and support improvised explosive device awareness and risk mitigation training – PSAs work in conjunction with IP's Office for Bombing Prevention by coordinating training and materials to SLTT partners to assist them in deterring, detecting, preventing, protecting against, and responding to improvised explosive device threats.

Learn more at https://www.dhs.gov/stakeholder-risk-assessment-mitigation for CSAs and https://www.dhs.gov/protective-security-advisors for PSAs.

Appendix E: Examples of Available Resources

#	Title	Type	CSF Category	CSF Function	Sector	Owner	Audience	Link	Summary
1	C^3 Voluntary Program (VP) SMB Toolkit	Guide	Risk Management Strategy	Identify	All	DHS	All Small Business Employees	https://www.us-cert.gov/ccubedvp/smb	This packet contains resources specially designed to help SMBs recognize and address their cybersecurity risks. Resources include talking points for business managers and leadership, steps to start evaluating your cybersecurity program, and a list of hands-on resources available to SMBs.
2	C^3VP Outreach and Messaging Kit	Guide	Awareness and Training	Protect	All	DHS	Small Business Leaders	https://www.us-cert.gov/sites/default/files/c3vp/smb/CCubedVP_Outreach_and_Messaging_Kit_SMB.pdf	Document to inform an organization's' partners about working with the C3VP.
3	Begin the Conversation: Understand the Threat Environment	Guide	Risk Management Strategy	Identify	All	DHS	Small Business Leaders	https://www.us-cert.gov/sites/default/files/c3vp/smb/Understanding_the_Threat_Landscape.pdf	Cyber threat environment introduction guide.
4	Cybersecurity for Startups	Guide	Awareness and Training	Protect	All	DHS	Small Business Leaders	https://www.us-cert.gov/sites/default/files/c3vp/smb/Cybersecurity_for_Startups_Slick_Sheet.pdf	Cybersecurity overview specifically for startups.

5	Small and Midsize Business Leadership Agenda	Guide	Awareness and Training	Protect	All	DHS	Small Business Leaders	https://www.us-cert.gov/sites/default/files/c3vp/smb/Leadership_Team_Agenda.pdf	Guidance for SMB leaders.
6	Hands-On Support for Small and Midsize Businesses	Guide	Awareness and Training	Protect	All	DHS	Small business stakeholders of all sizes and all sectors.	https://www.us-cert.gov/sites/default/files/c3vp/smb/Hands_On_Support.pdf	Overview of DHS hands-on resources to help stakeholders of all sizes address their cybersecurity needs.
7	Stop.Think.Connect. Small Business Resource Guide	Guide	Awareness and Training	Protect	All	National Cyber Security Alliance	All Small Business Employees	http://www.stcguide.com/explore/small-business/	The Stop.Think.Connect.™ campaign has an online Resource Guide specific to SMBs. The guide contains information from SMBs on mobile safety information, cybersecurity guidance for employees, and a small business tip card, among many other resources.
8	Stop.Think.Connect. Cybersecurity 101	Guide	Awareness and Training	Protect	All	DHS		https://www.dhs.gov/sites/default/files/publications/cybersecurity-101_4.pdf	Cybersecurity introduction guide.
9	Stop.Think.Connect. Mobile Security	Guide	Asset Management	Identify	All	DHS	Public Awareness	https://www.dhs.gov/sites/default/files/publications/Mobile%20Security%20One%20Pager_5.pdf	Stop.Think.Connect. Mobile security introduction guide.
10	Stop.Think.Connect. Basic	Tip Sheet	Awareness and Training	Protect	All	DHS	Public Awareness	https://staysafeonline.org/wp-content/uploads/2017/09	Tip sheet on cybersecurity best practices.

	Tips and Advice							/STOP.-THINK.-CONNECT.-Basic-Tips-Advice.pdf	
11	Stop.Think.Connect. Ransomware Facts & Tips	Tip Sheet	Awareness and Training	Protect	All	DHS	Public Awareness	https://staysafeonline.org/wp-content/uploads/2017/09/STOP.-THINK.-CONNECT.-Ransomware-Facts-Tips.pdf	Tip sheet designed to provide businesses with guidance to avoid and respond to Ransomware attacks.
12	Stop.Think.Connect. National Cybersecurity Awareness Campaign: Small Business Presentation	Presentation	Awareness and Training	Protect	All	DHS	Small Business Leaders	https://www.dhs.gov/sites/default/files/publications/Small%20Business%20Presentation.pdf	Cybersecurity overview for SMBs.
13	US-CERT (United States Computer Emergency Readiness Team)	Webpage	Awareness and Training	Identify	All	DHS	Public Awareness	https://www.us-cert.gov/security-publications	Publications from DHS that can help you with everything from setting up your first computer to understanding the nuances of emerging threats.
14	United States Computer Emergency Readiness Team (US-CERT	Webpage	Awareness and Training	Protect	All	DHS	All Businesses	https://www.us-cert.gov/related-resources	Identified resources on security organizations, vulnerability information, research, education, information sharing, and federal cyber policy.

15	DHS Cyber Resources	Webpage	Awareness and Training	Identify	All	DHS	All Businesses	https://www.dhs.gov/topic/cybersecurity	A starting point for how to navigate DHS's multiple responsibilities in cyberspace.
16	National Initiative for Cybersecurity Careers and Studies	Training Platform	Awareness and Training	Protect	All	DHS	Public Awareness	https://niccs.us-cert.gov/training	The National Incentive for Cybersecurity Careers and Studies Education and Training Catalog offers more than 3,000 cybersecurity-related courses throughout the country, both online and in person from over 125 different providers.
17	Small Business Administration Learning Center: Cybersecurity for Small Businesses	Online Course	Awareness and Training	Protect	All	SBA	Small Business Leaders	https://www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses	This 30 minute, self-paced training exercise provides an introduction to securing information in small businesses.
18	Protect Against Ransomware	Guide	Awareness and Training	Protect	All	SBA	All Businesses	https://www.sba.gov/managing-business/cybersecurity/protect-against-ransomware	A guide that offers tips and best practices to avoid falling victim to ransomware.
19	Social Media Cyber-Vandalism Toolkit	Guide	Recovery Planning	Recover	All	SBA	All Businesses	https://www.sba.gov/managing-business/cybersecurity/social-media-cyber-vandalism-toolkit	Developed by the SBA in conjunction with the U.S. GSA's SocialGov program, the Social Media Cyber-Vandalism Toolkit: Readiness, Recovery, Response provides

									guidance and security practices to small businesses.
20	Protect Your Customers	Tip Sheet	Awareness and Training	Protect	All	SBA	Small Business Leaders	https://staysafeonline.org/business-safe-online/resources/protect-your-customers	Tip sheet designed to help businesses increase customers' trust in their cybersecurity.
21	Small Business Innovation Research Program	Program	Awareness and Training	Protect	All	DHS	Small Business Leaders	https://www.dhs.gov/science-and-technology/sbir	The Small Business Innovation Research program, created in 1982 through the Small Business Innovation Development Act and reauthorized in 2011, is one of the largest public--private partnerships in the United States. This program encourages U.S. small businesses with fewer than 500 employees to provide quality research and to develop new processes, products, and technologies in support of the missions of the U.S. Government.
22	National Cyber Security Awareness Month	Program	Awareness and Training	Protect	All	DHS	Public Awareness	https://www.dhs.gov/national-cyber-security-awareness-month	National Cyber Security Awareness Month is designed to engage and educate public and private sector partners through events and initiatives to raise awareness about the importance of cybersecurity, provide them with tools and resources needed to stay safe

									online, and increase the resiliency of the Nation in the event of a cyber incident.
23	Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Assessment Program Overview	Webpage	Risk Assessment	Identify	All	DHS	All Businesses	https://ics-cert.us-cert.gov/Assessments	Overview of ICS-CERT's' assessment products.
24	Enhanced Cybersecurity Services (ECS)	Capability/Information Sharing	Security Continuous Monitoring	Detect	All	DHS	All Businesses	www.dhs.gov/ecs	ECS is an intrusion prevention service that helps protect U.S.-based companies, including small businesses, from unauthorized access, exploitation, and data exfiltration.
25	Cyber Information Sharing and Collaboration Program (CISCP)	Capability/Information Sharing	Awareness and Training	Detect/ Respond	All	DHS	All Businesses	https://www.dhs.gov/ciscp	A no-cost information sharing partnership between enterprises and DHS, CISCP creates shared situational awareness across critical infrastructure communities, enhances cybersecurity collaboration between DHS and critical infrastructure owners and operators, and leverages government and industry subject matter expertise to collaboratively

									respond to cybersecurity incidents.
27	5 Ways to Help Employees be #PrivacyAware	Tip Sheet	Awareness and Training	Protect	All	DHS	Small Business Leaders	https://staysafeonline.org/business-safe-online/resources/5-ways-to-help-employees-be-privacyaware	Tip sheet for businesses designed to help employees become aware of cybersecurity best practices.
28	Small Business Information/Cybersecurity Workshop	Presentation	Awareness and Training	Protect	All	NIST		http://csrc.nist.gov/groups/SMA/sbc/documents/sbc_workshop_presentation_2015_ver1.pdf	Cybersecurity workshop presentation for SMBs.
29	Small Business Information Security: The Fundamentals	Guide	Risk Assessment	Identify	All	NIST	Small Business Leaders	http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf	NIST developed this NISTIR as a reference guideline for small businesses. This document is intended to present the fundamentals of a small business information security program in non-technical language.
30	Small Business Corner	Webpage	Awareness and Training	Protect	All	NIST	Small Business Leaders	https://www.nist.gov/programs-projects/small-business-corner-sbc	Small Business Corner specific resource page.
31	Security and Privacy Controls for Federal Information Systems and Organizations	Guide	Access Control	Protect	All	NIST		http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf	NIST developed 800-53 as a reference guideline for controls to support the integration of information security and privacy into organizational processes including enterprise architecture, systems engineering, system

									development life cycle, and acquisition/procurement. Successful integration of security and privacy controls into ongoing organizational processes will demonstrate a greater maturity of security and privacy programs and provide a tighter coupling of security and privacy investments to core organizational missions and business functions.
32	NIST Cybersecurity Framework Reference Tool	Interactive Tool	Awareness and Training	Protect	All	NIST	All Businesses	https://www.nist.gov/cyberframework/csf-reference-tool	The Framework Core consists of five concurrent and continuous Functions - Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's' management of cybersecurity risk. The Framework Core then identifies underlying key Categories and Subcategories for each Function, and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory.

33	NIST Cybersecurity Framework – Industry Resources	Webpage	Awareness and Training	Protect	All	NIST	All Businesses	https://www.nist.gov/cyberframework/industry-resources	This is a listing of publicly available Framework resources. Resources include, but are not limited to: approaches, methodologies, implementation guides, mappings to the Framework, case studies, educational materials, Internet resource centers (e.g., blogs, document stores), example profiles, and other Framework document templates.
34	Federal Small Biz Cyber Planner	Custom Plan Generator	Awareness and Training	Protect	All	FCC	Small Business Leaders	https://www.fcc.gov/cyberplanner	This tool helps businesses create custom cybersecurity plans. The Small Biz Cyber Planner includes information on cyber insurance, advanced spyware, and how to install protective software.
35	Cyber Security Planning Guide	Guide	Risk Management Strategy	Identify	All	FCC	Small Business Leaders	https://www.dhs.gov/sites/default/files/publications/FCC%20Cybersecurity%20Planning%20Guide.pdf	This guide is designed to meet the specific needs of a business, using the FCC's customizable Small Biz Cyber Planner tool. This tool is designed for businesses that lack the resources to hire dedicated staff to protect their business, information, and customers from cyber threats.

36	Internet Security Essentials for Business 2.0	Guide	Risk Assessment	Identify	All	Chamber of Commerce		https://www.uschamber.com/CybersecurityEssentials	This guide for business owners, managers, and employees focuses on identifying common online risks, best practices for securing networks and information, and what to do when a cyber incident occurs.
37	Protecting Small Businesses	Webpage	Awareness and Training	Protect	All	Federal Trade Commission	Small Business Leaders	https://www.ftc.gov/SmallBusiness	Webpage with multiple resources for protecting small businesses from cybercrime.
38	Scam Alerts	Webpage		Protect	All	Federal Trade Commission	All Businesses	https://www.consumer.ftc.gov/scam-alerts	The latest information and practical tips from the nation's consumer protection agency.
39	Start with Security: A Guide for Business	Guide	Improvements	Recover	All	Federal Trade Commission	All Businesses	https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business	This guide collects lessons learned from the more than 50 law enforcement actions the FTC has announced so far in relation to data security settlements. These are settlements – no findings have been made by a court – and the specifics of the orders apply just to those companies. But learning about alleged lapses that led to law enforcement can help companies improve its practices.

40	Small Business	Webpage	Awareness and Training	Protect	All	Chamber of Commerce	Small Business Leaders	https://www.uschamber.com/members/small-business	Webpage with resource of small businesses.
41	Small Business Cyber Security Planning Guide	Guide	Risk Management Strategy	Identify	All	FCC		https://www.dhs.gov/sites/default/files/publications/FCC%20Cybersecurity%20Planning%20Guide.pdf	A tool for small businesses to create customized cyber security planning guides.
42	Best Practices for Victim Response and Reporting of Cyber Incidents	Guide	Response Planning	Response	All	DoJ	All Businesses	https://www.aba.com/Tools/Function/Fraud/Documents/doj-guidance-victim-response-reporting-cyber-incidents.pdf	Best practice guide for responding to and reporting cyber incidents.
43	The Cyber Threat to Small and Medium Sized Businesses is Real	Guide	Awareness and Training	Protect	All	ODNI		pdf	Infographic with SMB-related cyber threat information and data.
44	Cyber Threat - Recognition & Mitigation: A Guide for Small & Medium Sized Businesses (SMBs)	Guide	Mitigation	Response	All	ODNI		pdf	Infographic with suggested practices for SMBs to improve their cybersecurity.
45	Digital Blackmail as	Guide	Risk Management Strategy	Identify	All	ODNI		https://www.dni.gov/files/PE/Documents/Digital-	Article discussing Digital Blackmail and its growing risk to SMBs.

	an Emerging Tactic							Blackmail-as-an-Emerging-Tactic.pdf	
46	Going Bright: How the Internet of Things Could Revolutionize Intelligence Collection and Analysis	Guide	Awareness and Training	Protect	All	ODNI		https://www.dni.gov/files/PE/Documents/Internet-of-Things.pdf	Paper discussing the Internet of Things and its potential benefits to intelligence collection and analysis.

2

Appendix F: Glossary

America's Small Business Development Centers (ASBDC) - America's SBDC represents America's nationwide network of SBDCs – the most comprehensive small business assistance network in the United States and its territories. The mission of America's SBDC is to represent the interests of our members and their SBDCs, by promoting, informing, supporting, and continuously improving America's nationwide network of SBDCs.

Cyber Security Evaluation Tool - The Cyber Security Evaluation Tool is a DHS product that assists organizations in protecting their key national cyber assets. It was developed by cybersecurity experts under the direction of the DHS NCCIC. The tool provides users with a systematic and repeatable approach to assessing the security posture of their cyber systems and networks. It includes both high-level and detailed questions related to all industrial control and information technology systems.

Information Sharing and Analysis Center (ISAC) - ISACs 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.

Information Sharing and Analysis Organization (ISAO) - An ISAO is a group created to gather, analyze, and disseminate cyber threat information. Unlike ISACs, ISAOs are not directly tied to critical infrastructure sectors, as outlined in Presidential Policy Directive 21. Instead, ISAOs offer a more flexible approach to self-organized information sharing activities amongst communities of interest such as small businesses across sectors: legal, accounting, and consulting firms that support cross-sector clients, etc.

National Institute of Standards and Technology (NIST) Cybersecurity Framework - The Framework is voluntary guidance, based on existing standards, guidelines, and practices, for critical infrastructure organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders.

Small Business Concern – An enterprise that: (i) is independently owned and operated; (ii) is not dominant in its field of operations; and (iii) is within the applicable size standard for its industry.

Small Business Development Center (SBDC) – SBDCs are often university-based centers sponsored by the SBA for the delivery of joint government, academic, and private sector services for the benefit of small business.

Appendix G: Acronyms

Acronym	Definition
AIS	Automated Indicator Sharing
ASBDC	America's Small Business Development Center
C^3	Critical Infrastructure Cyber Community Voluntary Program
CERTs	Computer Emergency Response Teams
CIS	Center for Internet Security
CISA	(DHS) Cybersecurity and Infrastructure Security Agency
CISCP	Cyber Information Sharing and Collaboration Program
CRR	Cyber Resilience Review
CSA	Cyber Security Advisor
DHS	Department of Homeland Security
DoC	Department of Commerce
DoJ	Department of Justice
ECS	Enhanced Cybersecurity Services
EO	Executive Order
HIRT	Hunt and Incident Response Team
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FTC	Federal Trade Commission
FY	Fiscal Year
GSA	General Services Administration
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IDT	Identity Theft
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
IP	Office of Infrastructure Protection

NCCIC	National Cybersecurity and Communications Integration Center
NCSA	National Cyber Security Alliance
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
NSSE	National Special Security Events
ODNI	Office of the Director of National Intelligence
PSA	Protective Security Advisor Program
SBA	Small Business Administration
SBDC	Small Business Development Center
SEAR	Special Event Activity Rating
SMB	Small and Medium-Sized Business
SLTT	State, Local, Tribal, and Territorial
US-CERT	United States Computer Emergency Readiness Team