SBA
U.S. Small Business Administration

MANAGEMENT AND TECHNICAL ASSISTANCE PROGRAM
7(j) TRAINING

Cybersecurity

Beginning and Intermediate Training (10 total courses)

Eligible participants for this free training will learn critical cybersecurity concepts, approaches to protecting their resources and intellectual property, and mandatory federal contracting requirements for both prime and sub-tier subcontractors. Each course is approximately 1 hour.

Date: 10/30/2017 - 1/5/2018 (See schedule attached)

Time: a.m. - p.m.

Location: Interactive web-based training at:

https://synergysolutions.talentlms.com/

YOU WILL LEARN:

- Beginning level training modules 1-5 cover basic cybersecurity awareness and current cyber risks to federal contractors and small businesses.
- Intermediate level modules 6-10 cover more advanced cybersecurity and information assurance requirements, federal policy compliance, assessment areas, and credit card transaction data.
- Eligible 7(j) participants completing modules 1-10 sequentially will be provided 30-day access to an assessment tool that they can immediately use to assess their company's cybersecurity maturity.
- Schedule includes 6 NEW individual "How To" courses in November and December 2017.
- A detailed summary of classes and training calendar are attached.

REGISTRATION REQUIRED:

Contact Synergy at https://synergysolutions.talentlms.com/ for User ID assignment and course registration access. Courses are subject to a maximum of 20 participants and are listed are in Eastern Time.

For more Information about the 7(j) Program, please contact your SBA District Office. You can find local office information at www.sba.gov/tools/local-assistance.

Training provided by:

Synergy Solutions inc

SBA Cooperative Agreement contract # SBAHQ-16-D-0009
This project is funded by a Cooperative Agreement from the U.S. Small Business Administration (SBA). SBA's funding should not be construed as an endorsement of any products, opinions, or services. All SBA-funded projects are extended to the public on a nondiscriminatory basis

Reasonable accommodations for persons with disabilities will be made if requested at least two weeks in advance. Please contact:

https://synergysolutions.talentlms.com/

SBA CYBERSECURITY TRAINING SCHEDULE – NATIONWIDE

OCTOBER 30, 2017 – JANUARY 5, 2018

Beginning (Mods 1-5) and Intermediate (Mods 6-10) courses/modules are required to be taken in sequential order (1, 2, 3….9, 10). Participants are encouraged to plan for future classes and entry is guaranteed if participant attends previous pre-requisite course and demonstrates understanding in post-module quizzes. Formal enrollment of courses will be processed by the LMS Administrator only after previous course is completed so participants should not be alarmed that they cannot register for all courses at one time. The Cybersecurity Tool will be released to 7(j) participants after all 10 courses/modules are completed. NEW Classes (red text) are individual stand-alone courses; participants may benefit more if Beginning & Intermediate modules 1-10 are taken first.

MON	TUES	WED	THURS	FRI
OCT 30	**31** 2-3 pm ET: MOD 9 3:30 – 4:30 pm ET: MOD 10 *Tool Open (30 days)*	**NOV 1** 2-3 pm ET: MOD 1 3:30 – 4:30 pm ET: MOD 2	**2** 2-3 pm ET: MOD 3 3:30 – 4:30 pm ET: MOD 4	**3**
6	**7** 2-3 pm ET: MOD 1 3:30 – 4:30 pm ET: MOD 2	**8** 2-3 pm ET: MOD 5 3:30 – 4:30 pm ET: MOD 6	**9** 2-3 pm ET: MOD 3 3:30 – 4:30 pm ET: MOD 4	**10** 10-11 am ET: MOD 7 11:30 am-12:30 pm ET: MOD 8
13	**14** 2-3 pm ET: MOD 5 3:30 – 4:30 pm ET: MOD 6	**15** 2-3 pm ET: MOD 9 3:30 – 4:30 pm ET: MOD 10 *Tool Open (30 days)*	**16** 2-3 pm ET: MOD 7 3:30 – 4:30 pm ET: MOD 8	**17** ***NEW Classes*** 10-11 am ET: Secure Your Devices 11:30 am-12:30 pm ET: Secure Your Online Life
20	**21** 2-3 pm ET: MOD 9 3:30 – 4:30 pm ET: MOD 10 *Tool Open (30 days)*	**22** ***NEW Classes*** 2-3 pm ET: Evaluate your Cybersecurity Readiness 3:30 – 4:30 pm ET: Cyber Incident Response	**23** ***THANKSGIVING HOLIDAY***	**24**
27	**28** 2-3 pm ET: MOD 1 3:30 – 4:30 pm ET: MOD 2	**29** 2-3 pm ET: MOD 3 3:30 – 4:30 pm ET: MOD 4	**30** ***NEW Classes*** 2-3 pm ET: Cybersecurity Plan 3:30 – 4:30 pm ET: Fed Breach Notification Requirements	**DEC 1** 10-11 am ET: MOD 5 11:30 am-12:30 pm ET: MOD 6

Funded through a contract with the U.S. Small Business Administration. SBA's funding is not an endorsement of the contractor or any products, opinions, or services. All SBA programs are extended to the public on a non-discriminatory basis.

SBA CYBERSECURITY TRAINING SCHEDULE – NATIONWIDE

OCTOBER 30, 2017 – JANUARY 5, 2018

Beginning (Mods 1-5) and Intermediate (Mods 6-10) courses/modules are required to be taken in sequential order (1, 2, 3….9, 10). Participants are encouraged to plan for future classes and entry is guaranteed if participant attends previous pre-requisite course and demonstrates understanding in post-module quizzes. Formal enrollment of courses will be processed by the LMS Administrator only after previous course is completed so participants should not be alarmed that they cannot register for all courses at one time. The Cybersecurity Tool will be released to 7(j) participants after all 10 courses/modules are completed. NEW Classes (red text) are individual stand-alone courses; participants may benefit more if Beginning & Intermediate modules 1-10 are taken first.

MON	TUES	WED	THURS	FRI
DEC 4	**5** 2-3 pm ET: MOD 1 3:30 – 4:30 pm ET: MOD 2	**6** 2-3 pm ET: MOD 3 3:30 – 4:30 pm ET: MOD 4	**7** 2-3 pm ET: MOD 7 3:30 – 4:30 pm ET: MOD 8	**8** 10-11 am ET: MOD 9 11:30 am-12:30 pm ET: MOD 10 *Tool Open (30 days)*
11	**12** 2-3 pm ET: MOD 5 3:30 – 4:30 pm ET: MOD 6	**13** 2-3 pm ET: MOD 7 3:30 – 4:30 pm ET: MOD 8	**14** 2-3 pm ET: MOD 1 3:30 – 4:30 pm ET: MOD 2	**15 *NEW Classes*** 10-11 am ET: Evaluate you Cybersecurity Readiness 11:30 – 12:30 pm ET: Cyber Incident Response
18	**19** 2-3 pm ET: MOD 3 3:30 – 4:30 pm ET: MOD 4	**20** 2-3 pm ET: MOD 9 3:30 – 4:30 pm ET: MOD 10 *Tool Open (30 days)*	**21** 2-3 pm ET: MOD 5 3:30 – 4:30 pm ET: MOD 6	**22 *NEW Classes*** 10-11 am ET: Cybersecurity Plan 11:30 am-12:30 pm ET: Fed Breach Notification Requirements
25 ***CHRISTMAS HOLIDAY***	**26**	**27**	**28**	**29**
JAN 1 ***NEW YEAR'S HOLIDAY***	**2**	**3 *NEW Classes*** 2-3 pm ET: Secure Your Devices 3:30 - 4:30 pm ET: Secure Your Online Life	**4** 2-3 pm ET: MOD 7 3:30 – 4:30 pm ET: MOD 8	**5** 10-11 am ET: MOD 9 11:30 am-12:30 pm ET: MOD 10 *Tool Open (30 days)*

U.S. Small Business Administration

Funded through a contract with the U.S. Small Business Administration. SBA's funding is not an endorsement of the contractor or any products, opinions, or services. All SBA programs are extended to the public on a non-discriminatory basis.

COURSE SYNOPSES
SBA CYBERSECURITY TRAINING

Courses build on previously taught concepts so classes must be taken in consecutive order. Each class size has a minimum of 5 and maximum of 20 participants to allow optimum interaction between the instructor and participants. Classes that do not meet the minimum number of participants may be rescheduled or cancelled.

BASIC CYBERSECURITY MODULES (1-5)

Module 1. Why Cybersecurity? – In this module, we'll discuss what cybersecurity means for your company, employees, partners and customers. We'll consider what makes your company vulnerable, how data breaches occur and some steps you can take to protect your company and your data. Finally, we'll explore some of the laws and contracting requirements that specifically apply to companies doing business with the Federal Government or their prime contractors.

Module 2. Cybersecurity Basics – This module is specifically focused on fundamental concepts of cybersecurity. We'll discuss the goals, objectives and essential objectives of cybersecurity programs and how successful programs are implemented. Finally, we'll consider some specific foundational activities like good password discipline, effective strategies for backing up data and elements of effective cybersecurity policies to help protect your business assets and reputation.

Module 3. Endpoint Security – In this module, you'll learn about how endpoint devices such as laptops, desktops, tablet computers and mobile devices can offer cybercriminals a gateway into your company's networks and data. We'll discuss the various types of endpoint devices, what makes them vulnerable to exploit by cybercriminals and how to protect them from attack. We'll also discuss one of the basic concepts of cybersecurity – defense-in-depth.

Module 4. Network Security – Securing your network is one of the basic tasks of providing cybersecurity for your company. In this module, we'll discuss what it takes to properly secure a business network, explore the various threats networks commonly face, and how the concept of defense-in-depth applies to protecting your network. Finally, we'll consider specific network protection tools, such as Intrusion Detection/Intrusion Prevention Systems (IDS/IPS), firewalls, Network Access Control programs and anti-virus/anti-malware systems.

Module 5. Data Security – The bottom line of cybersecurity is providing protection for your company's data and that of your customers and partners. This module will discuss why protecting data should be at the heart of your cybersecurity program, the types of data you are responsible for and threats to that data. We'll introduce and discuss the concept of individual cyber hygiene and discuss a case study of one incident where data security broke down and the serious consequences that followed.

U.S. Small Business Administration

Funded through a contract with the U.S. Small Business Administration. SBA's funding is not an endorsement of the contractor or any products, opinions, or services. All SBA programs are extended to the public on a non-discriminatory basis.

INTERMEDIATE CYBERSECURITY MODULES (6-10)

Module 6. Security Frameworks and Standards - In this module, you will learn about cybersecurity standards and discuss several frameworks that are relevant to cybersecurity. We'll explore U.S. and international cybersecurity frameworks, including a detailed discussion of the National Institute of Standards and Technology (NIST) framework and cybersecurity standards specific to federal government contractors and to entities that process or store credit card data.

Module 7. Laws and Regulatory Compliance - The Internet has often been equated to the lawlessness of the Wild West, but the reality is much different. While many types of behavior flourish on the Internet, nations and international bodies are slowly developing legal and regulatory frameworks to help bring order to the chaos. In this module, we'll discuss State, Federal and international laws and regulations you and your company will be expected to follow when you have a data breach or possess and process your customer's or employee's sensitive data. Finally, we'll explore the expectations various groups (e.g., the public, customers, media) will have of you if your company suffers a data breach.

Module 8. Breaches, Security Crises and Incident Response - In this module, we'll conduct a detailed exploration of the targets, motivations and techniques of hackers, as well as various types of common attacks. We'll transition to discussing the incident response cycle and cyber investigations. We'll conclude with new developments in cybersecurity such as the rise of the use of cyber threat intelligence and how third-parties who handle or process your data may prove to be a previously unconsidered area of risk.

Module 9. Prevention and Remediation - Preventing data breaches and incidents is a subject that is often a source of great discussion. In this module, we'll consider some basic truths about cybersecurity and data breaches, as well as some limitations of your cybersecurity efforts. We'll discuss how not to be a data breach victim, as well as outline some steps you can take to decrease or mitigate your company's risk of a data breach. Finally, we'll explore remediation steps you need to take should a breach occur to quickly recover and lessen the chances of reoccurrence.

Module 10. Management Responsibilities and the Cyber Future - As the CEO or senior leader of your business, you have specific requirements when it comes to cybersecurity. This module will explore how executives must take responsibility for their company cybersecurity efforts and support and oversee these efforts. We'll discuss specific threats to small businesses, such as ransomware, phishing and theft of data and end with a review of the techniques cybercriminals to steal credit card data.

Cybersecurity Assessment Tool: Once a participant receives credit for passing all ten (10) cybersecurity training modules, they will be granted access to the Small Business Cybersecurity Assessment Tool 1.0 for 30 days. The tool will help assess their business's cyber maturity and receive improvement recommendations to get to the next step for their business.

U.S. Small Business Administration

Funded through a contract with the U.S. Small Business Administration. SBA's funding is not an endorsement of the contractor or any products, opinions, or services. All SBA programs are extended to the public on a non-discriminatory basis.

CYBERSECURITY "HOW TO" CLASSES – SYNOPSES

These classes are designed to expand upon specific topics covered in the SBA Cybersecurity Basic and Intermediate courses. Each class will consist of a one hour session that delves deeper into the details of specific topics of interest to cybersecurity course students.

Building a Security Plan

This class will cover details on how to develop a cybersecurity plan for a small business, including online references, sample plans and various items of interest in security planning. Students will be expected to complete their own small business security plan based on the templates and information provided in the class. These plans will be reviewed by the instructors and returned with comments and suggestions.

Securing Devices

This class will provide detailed discussion on how to harden and improve security settings on common devices we all use, such as laptops, desktops, tablet computers, home routers and smart phones. Securing popular operating systems (Android, Microsoft Windows 10, and IOS (iPhone) will be covered in detail, as will common malware and important current threats against each.

Securing your Online Life

This class will discuss how to secure both a small business' online presence and the online life of the individual participant. Improving security settings for common social media applications, such as Facebook and Twitter will be covered, as well as discussion of tools to help make daily online life easier and more secure

Responding to Incidents

Responding effectively to cyber incidents, including notifications and root cause determinations, can be some of the most daunting experiences in the life of a small business. This class will discuss basic concepts in response, investigations, and determination of root cause in a suspected or actual cyber incident. Taught by experts experienced in leading businesses through cyber incidents, this class will also include hints and inside information on dealing with customers, employees, regulators and law enforcement during the stress and uncertainty that accompanies a serious cyber incident.

Evaluating your Readiness

How ready is your small business to deal with a serious cyber incident? Like many other aspects of a small business' daily life, the possibility of a serious cyber incident should be considered and planned for BEFORE it happens. This class will help participants think through how they need to respond during various phases of different types of cyber incidents. It will also discuss the elements of a good plan for responding to incidents and help participants prepare simple incident response plans for their own small businesses.

Federal Breach Notification Requirements

Federal government contractors who handle sensitive unclassified or personal data for the Federal government recently became responsible for reporting incidents involving potential or actual loss or compromise of that data. These requirements, along with requirements for cybersecurity planning by contractors, have been incorporated into the Defense Federal Acquisition Regulation (DFAR) and will most likely be made part of the overall Federal Acquisition Regulation (FAR) soon. This will require cybersecurity planning for almost all Federal contractors. This class will discuss the specific nuances of breach reporting for Federal contractors and give participants a glimpse at what changes to expect to Federal contracting procedures regarding cybersecurity.

U.S. Small Business Administration

Funded through a contract with the U.S. Small Business Administration. SBA's funding is not an endorsement of the contractor or any products, opinions, or services. All SBA programs are extended to the public on a non-discriminatory basis.