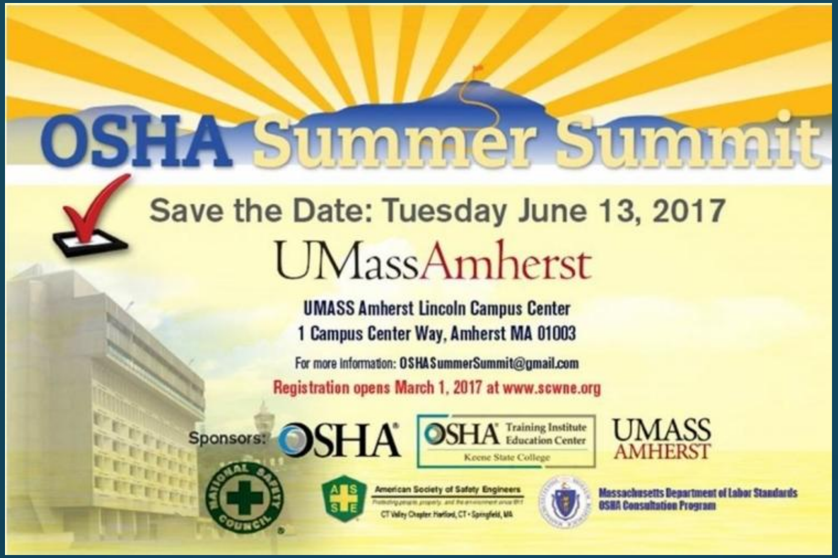


OSHA Summer Summit

Save the Date: Tuesday June 13, 2017

UMassAmherst

UMASS Amherst Lincoln Campus Center
1 Campus Center Way, Amherst MA 01003

For more information: OSHASummerSummit@gmail.com

Registration opens March 1, 2017 at www.scwne.org

Sponsors: OSHA® | OSHA® Training Institute Education Center, Keene State College | UMASS AMHERST | National Safety Council | American Society of Safety Engineers, Protecting people, property, and the environment since 1911, CT Valley Chapter: Hartford, CT • Springfield, MA | Massachusetts Department of Labor Standards OSHA Consultation Program

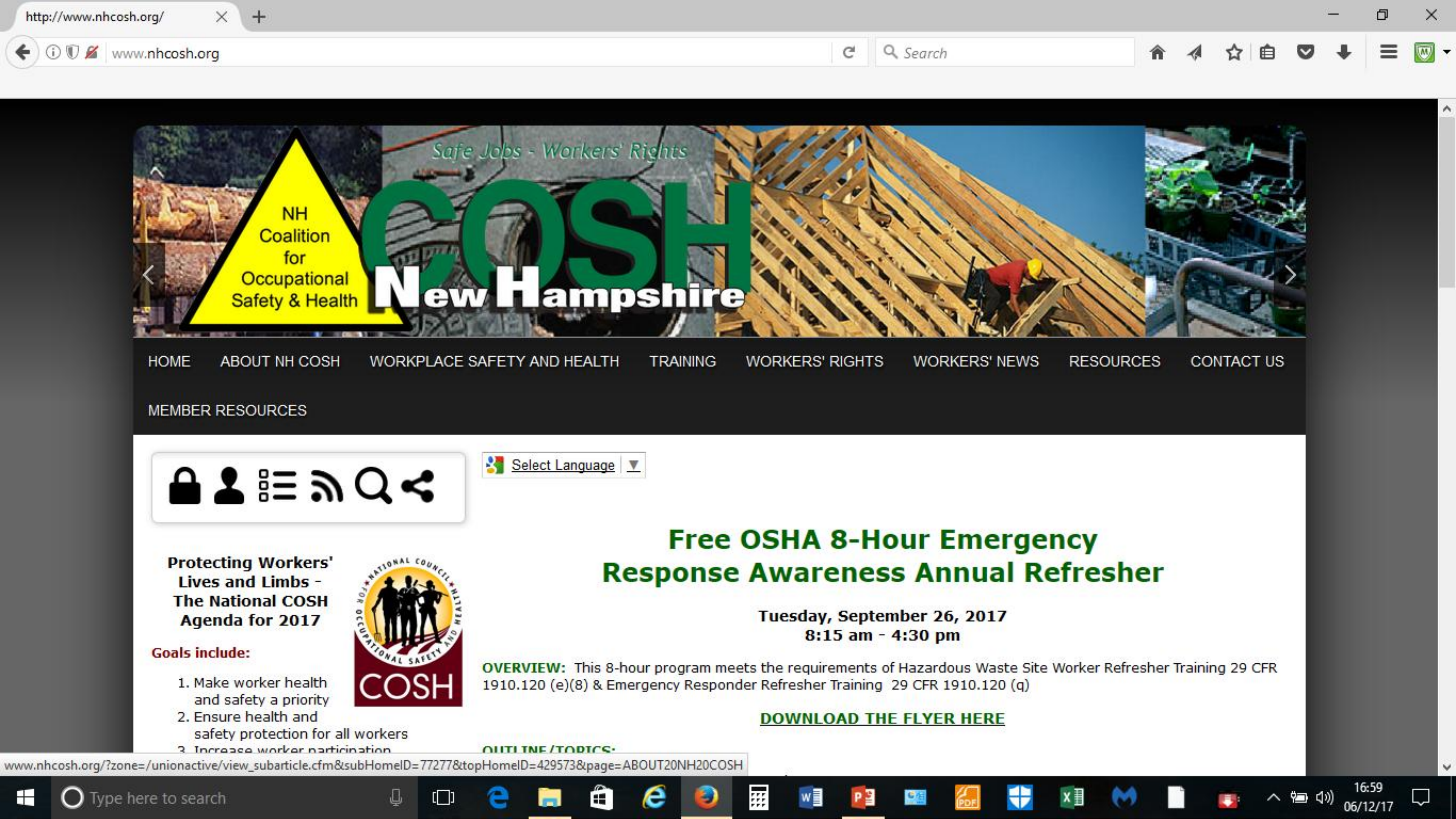
TNEC

Health and Safety Training

Is your Business at Risk? Terrorism in the Workplace

Housekeeping

- Exits
- Rally points
- Cell phones
- Facilities


http://www.nhcosh.org/
www.nhcosh.org
Search
Safe Jobs - Workers' Rights
NH Coalition for Occupational Safety & Health
COSH
New Hampshire
HOME
ABOUT NH COSH
WORKPLACE SAFETY AND HEALTH
TRAINING
WORKERS' RIGHTS
WORKERS' NEWS
RESOURCES
CONTACT US
MEMBER RESOURCES
Select Language
NATIONAL COUNCIL FOR OCCUPATIONAL SAFETY AND HEALTH
COSH
www.nhcosh.org/?zone=/unionactive/view_subarticle.cfm&subHomeID=77277&topHomeID=429573&page=ABOUT20NH20COSH
Type here to search
16:59
06/12/17

Protecting Workers' Lives and Limbs - The National COSH Agenda for 2017

Goals include:

1. Make worker health and safety a priority
2. Ensure health and safety protection for all workers
3. Increase worker participation

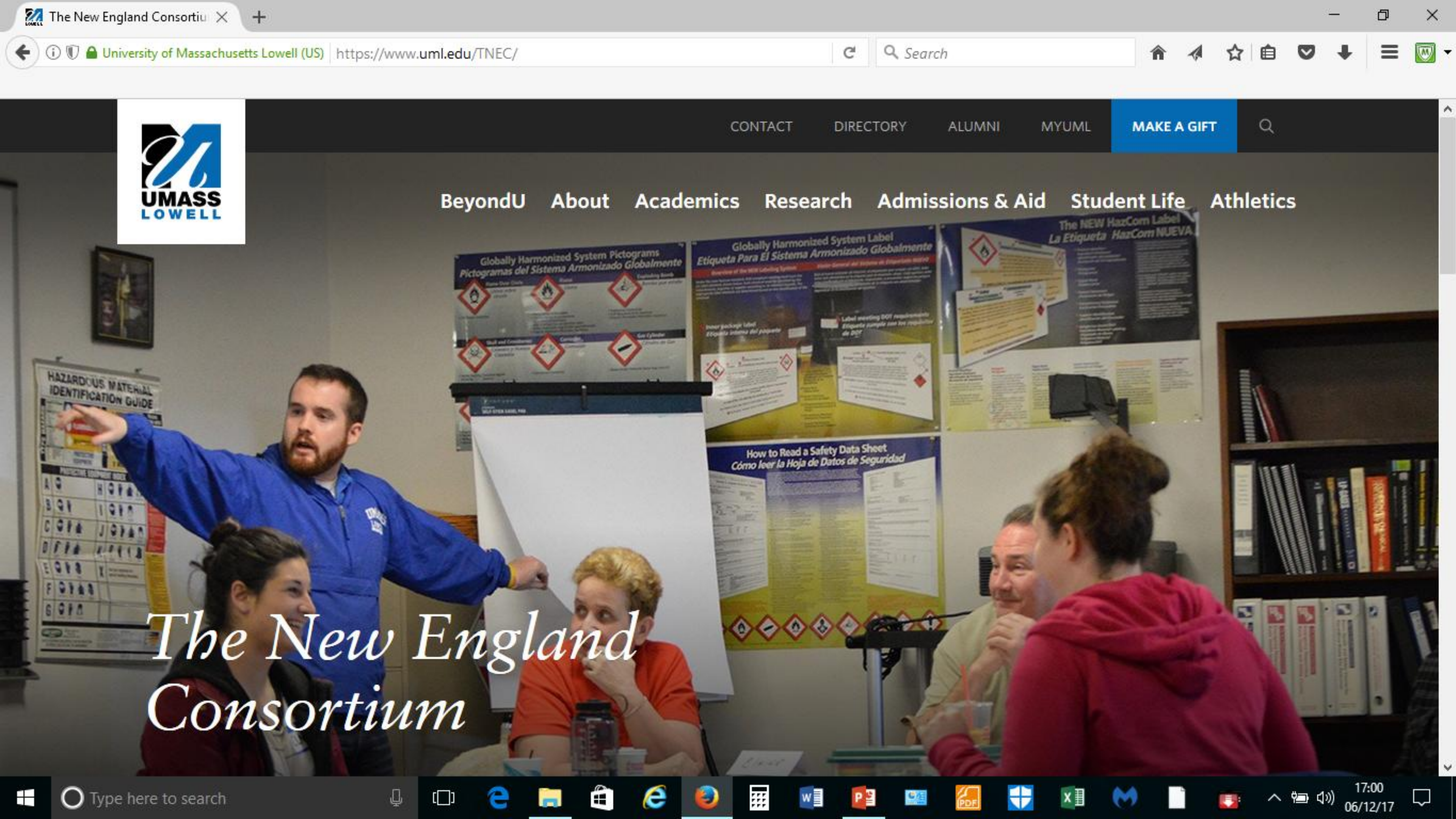
Free OSHA 8-Hour Emergency Response Awareness Annual Refresher

Tuesday, September 26, 2017
8:15 am - 4:30 pm

OVERVIEW: This 8-hour program meets the requirements of Hazardous Waste Site Worker Refresher Training 29 CFR 1910.120 (e)(8) & Emergency Responder Refresher Training 29 CFR 1910.120 (q)

DOWNLOAD THE FLYER HERE

OUTLINE/TOPICS:


The New England Consortiu
University of Massachusetts Lowell (US)
https://www.uml.edu/TNEC/
Search
UMASS LOWELL
CONTACT
DIRECTORY
ALUMNI
MYUML
MAKE A GIFT
BeyondU
About
Academics
Research
Admissions & Aid
Student Life
Athletics
Globally Harmonized System Pictograms
Pictogramas del Sistema Armonizado Globalmente
Globally Harmonized System Label
Etiqueta Para El Sistema Armonizado Globalmente
The NEW HazCom Label
La Etiqueta HazCom NUEVA
How to Read a Safety Data Sheet
Cómo leer la Hoja de Datos de Seguridad
HAZARDOUS MATERIAL IDENTIFICATION GUIDE
Type here to search
17:00
06/12/17

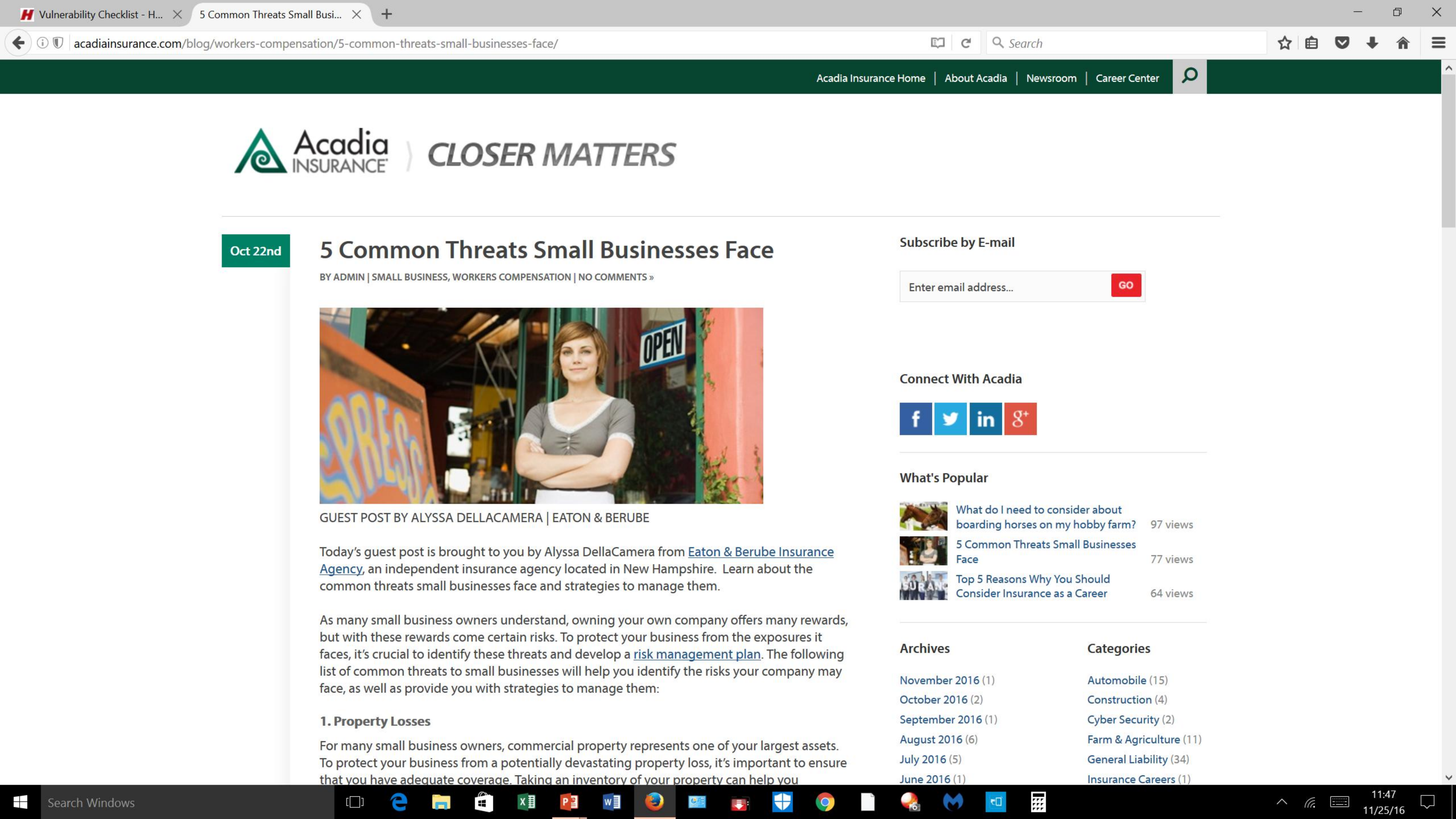
The New England Consortium

Agenda

- Threats/Tactical actions
- Vulnerability assessment
- Prevention/Protection/Information sources

Business Threats

- Insurance companies list threats to businesses ranging from property losses through electronic data breaches.
- Threat assessment has transcended from the traditional view to encompass both environmental and deliberate causes.
  - The term “all-hazards” is now considered de riguer in the emergency response community.
  - Domestic and international groups would harm and have harmed the US for a variety of reasons.


Vulnerability Checklist - H...
5 Common Threats Small Busi...
acadiainsurance.com/blog/workers-compensation/5-common-threats-small-businesses-face/
Search
Acadia Insurance Home | About Acadia | Newsroom | Career Center
Acadia INSURANCE
CLOSER MATTERS
Search Windows
11:47
11/25/16

Oct 22nd

5 Common Threats Small Businesses Face

BY ADMIN | SMALL BUSINESS, WORKERS COMPENSATION | NO COMMENTS »

GUEST POST BY ALYSSA DELLACAMERA | EATON & BERUBE

Today's guest post is brought to you by Alyssa DellaCamera from Eaton & Berube Insurance Agency, an independent insurance agency located in New Hampshire. Learn about the common threats small businesses face and strategies to manage them.

As many small business owners understand, owning your own company offers many rewards, but with these rewards come certain risks. To protect your business from the exposures it faces, it's crucial to identify these threats and develop a risk management plan. The following list of common threats to small businesses will help you identify the risks your company may face, as well as provide you with strategies to manage them:

1. Property Losses

For many small business owners, commercial property represents one of your largest assets. To protect your business from a potentially devastating property loss, it's important to ensure that you have adequate coverage. Taking an inventory of your property can help you

Subscribe by E-mail

Enter email address... GO

Connect With Acadia

f | t | in | g+

What's Popular

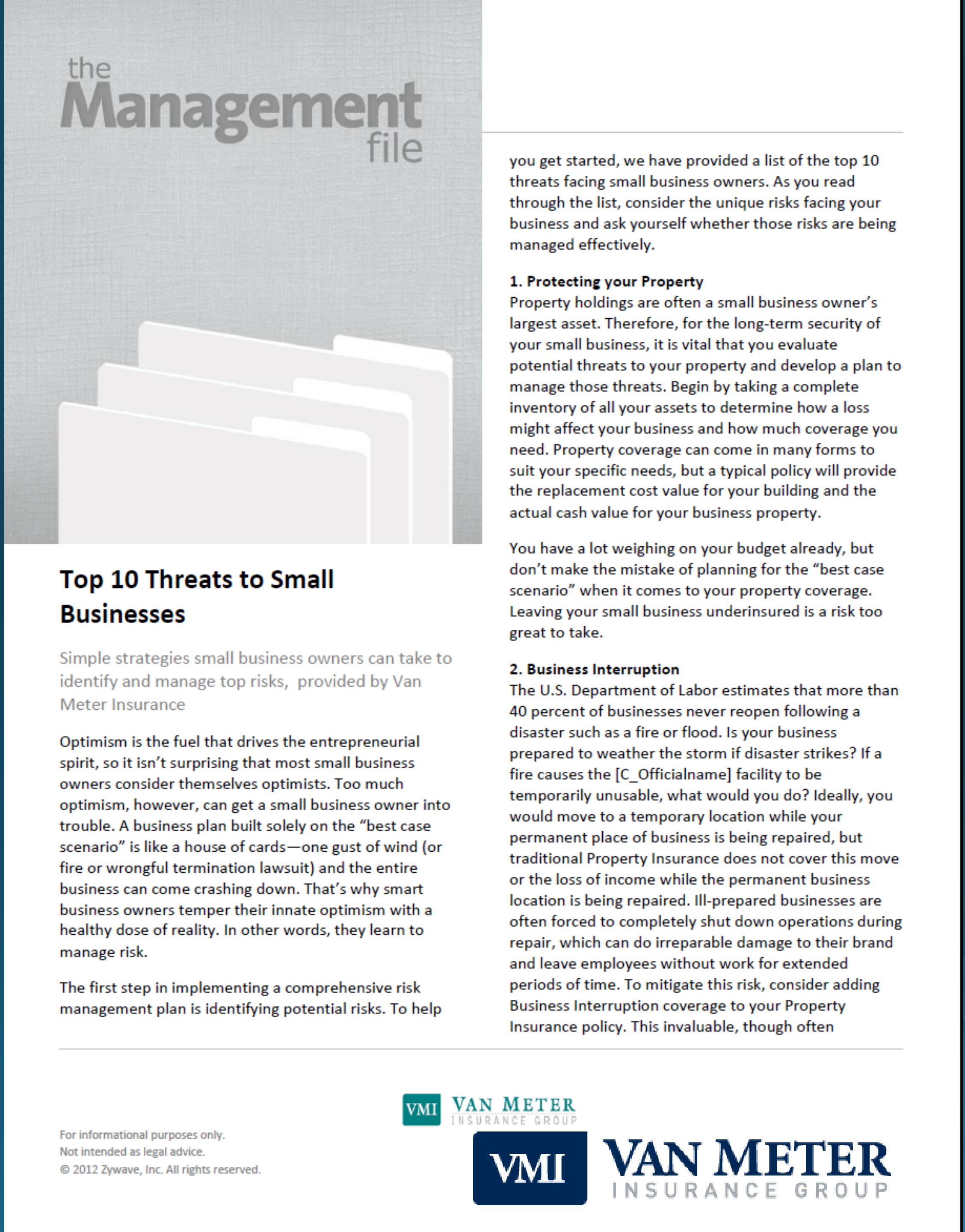
What do I need to consider about boarding horses on my hobby farm?	97 views
5 Common Threats Small Businesses Face	77 views
Top 5 Reasons Why You Should Consider Insurance as a Career	64 views

Archives

November 2016 (1)
October 2016 (2)
September 2016 (1)
August 2016 (6)
July 2016 (5)
June 2016 (1)

Categories

Automobile (15)
Construction (4)
Cyber Security (2)
Farm & Agriculture (11)
General Liability (34)
Insurance Careers (1)



the Management file

Top 10 Threats to Small Businesses

Simple strategies small business owners can take to identify and manage top risks, provided by Van Meter Insurance

Optimism is the fuel that drives the entrepreneurial spirit, so it isn't surprising that most small business owners consider themselves optimists. Too much optimism, however, can get a small business owner into trouble. A business plan built solely on the "best case scenario" is like a house of cards—one gust of wind (or fire or wrongful termination lawsuit) and the entire business can come crashing down. That's why smart business owners temper their innate optimism with a healthy dose of reality. In other words, they learn to manage risk.

The first step in implementing a comprehensive risk management plan is identifying potential risks. To help you get started, we have provided a list of the top 10 threats facing small business owners. As you read through the list, consider the unique risks facing your business and ask yourself whether those risks are being managed effectively.

1. Protecting your Property

Property holdings are often a small business owner's largest asset. Therefore, for the long-term security of your small business, it is vital that you evaluate potential threats to your property and develop a plan to manage those threats. Begin by taking a complete inventory of all your assets to determine how a loss might affect your business and how much coverage you need. Property coverage can come in many forms to suit your specific needs, but a typical policy will provide the replacement cost value for your building and the actual cash value for your business property.

You have a lot weighing on your budget already, but don't make the mistake of planning for the "best case scenario" when it comes to your property coverage. Leaving your small business underinsured is a risk too great to take.

2. Business Interruption

The U.S. Department of Labor estimates that more than 40 percent of businesses never reopen following a disaster such as a fire or flood. Is your business prepared to weather the storm if disaster strikes? If a fire causes the [C_Officialname] facility to be temporarily unusable, what would you do? Ideally, you would move to a temporary location while your permanent place of business is being repaired, but traditional Property Insurance does not cover this move or the loss of income while the permanent business location is being repaired. Ill-prepared businesses are often forced to completely shut down operations during repair, which can do irreparable damage to their brand and leave employees without work for extended periods of time. To mitigate this risk, consider adding Business Interruption coverage to your Property Insurance policy. This invaluable, though often

For informational purposes only.
Not intended as legal advice.

VMI VAN METER INSURANCE GROUP

VMI VAN METER INSURANCE GROUP

Critical Infrastructure/Key Resources

- Presidential Policy Directive 21 enumerated 16 Sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

SSA Definition

- The term "Sector-Specific Agency" (SSA) means the Federal department or agency designated under this directive to be responsible for:
  - Providing institutional knowledge
  - And specialized expertise as well as
  - Leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment.

CI/KR Sectors

- **Chemical:**
  - Sector-Specific Agency: Department of Homeland Security
- **Commercial Facilities:**
  - Sector-Specific Agency: Department of Homeland Security
- **Communications:**
  - Sector-Specific Agency: Department of Homeland Security

CI/KR Sectors

- Critical Manufacturing:
  - Sector-Specific Agency: Department of Homeland Security
- Dams:
  - Sector-Specific Agency: Department of Homeland Security
- Defense Industrial Base:
  - Sector-Specific Agency: Department of Defense
- Emergency Services:
  - Sector-Specific Agency: Department of Homeland Security

CI/KR Sectors

- Energy:
  - Sector-Specific Agency: Department of Energy
- Financial Services:
  - Sector-Specific Agency: Department of the Treasury
- Food and Agriculture:
  - Co-Sector-Specific Agencies: U.S. Department of Agriculture and Department of Health and Human Services

CI/KR Sectors

- Government Facilities:
  - Co-Sector-Specific Agencies: Department of Homeland Security and General Services Administration
- Healthcare and Public Health:
  - Sector-Specific Agency: Department of Health and Human Services
- Information Technology:
  - Sector-Specific Agency: Department of Homeland Security

CI/KR Sectors

- **Nuclear Reactors, Materials, and Waste:**
  - Sector-Specific Agency: Department of Homeland Security
- **Transportation Systems:**
  - Co-Sector-Specific Agencies: Department of Homeland Security and Department of Transportation
- **Water and Wastewater Systems:**
  - Sector-Specific Agency: Environmental Protection Agency

Private Sector CI/KR Impact

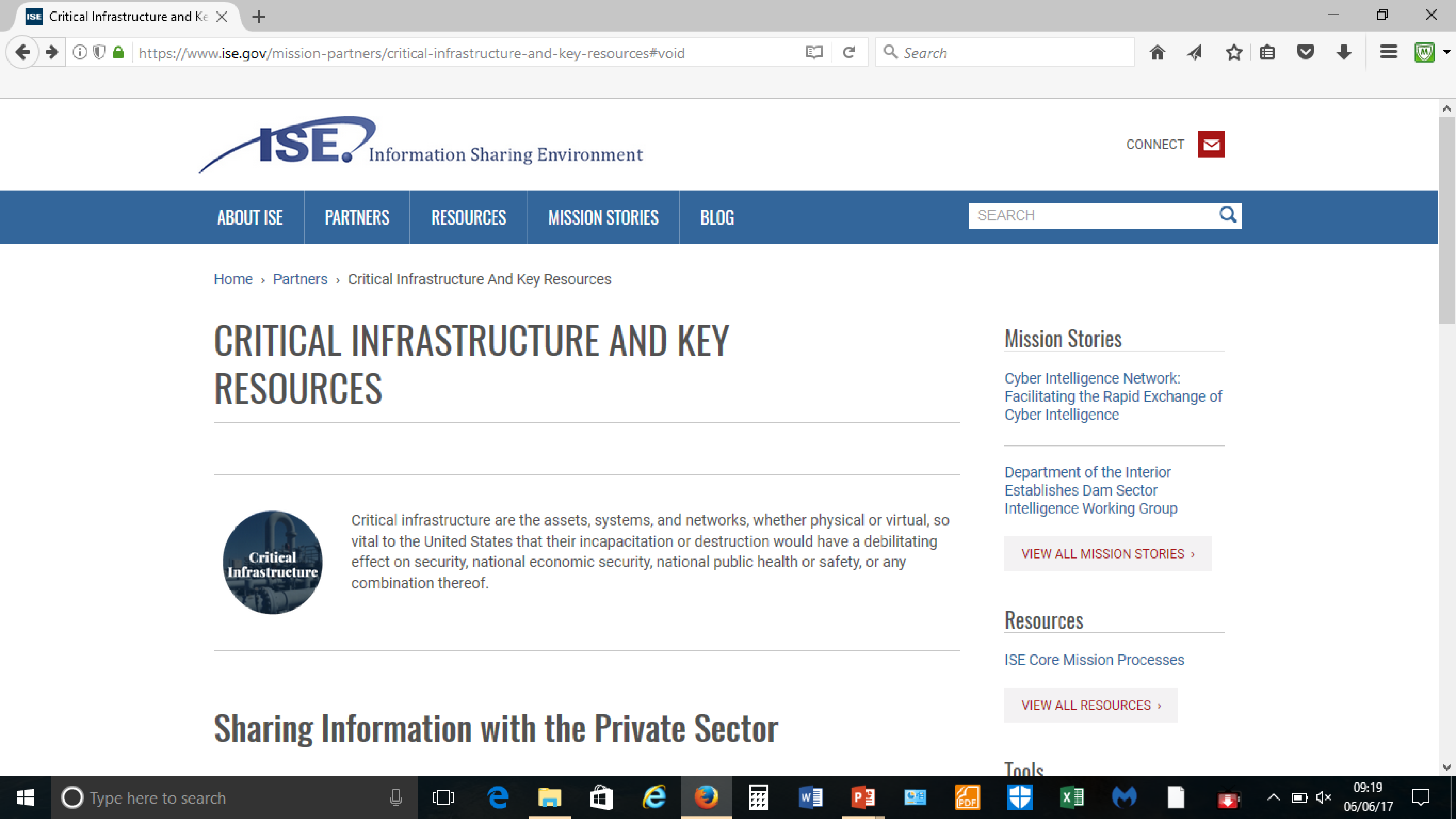
- Private-sector CI/KR owners and operators are responsible at the corporate and individual facility levels for risk and incident management planning, security, and preparedness investments.
- Other activities that form part of business and continuity of operations planning activities include:
  - Developing and revising business continuity and emergency management plans to address direct effects of incidents and critical dependencies and interdependencies at sector, enterprise, and facility levels.
  - Building increased resiliency, backup capabilities, and redundancy into business processes and systems.

Private Sector CI/KR Impact

- Maintaining coordination with incident management, information-sharing, and CI/KR protection programs.
- Reporting CI/KR status using established mechanisms for inclusion in the national common operating picture (COP).
- Developing and coordinating CI/KR protective and emergency-response actions, plans, and programs.

Private Sector CI/KR Impact

- Guarding against insider threats.
- Providing technical expertise to DHS, SSAs, ESFs, and other Federal, State, tribal, and local entities.
- Identifying CI/KR and prioritizing related protection and restoration activities.


Critical Infrastructure and Ke
https://www.ise.gov/mission-partners/critical-infrastructure-and-key-resources#void
Search
Type here to search
09:19
06/06/17

ISE. Information Sharing Environment

CONNECT

ABOUT ISE | PARTNERS | RESOURCES | MISSION STORIES | BLOG

SEARCH

Home › Partners › Critical Infrastructure And Key Resources

CRITICAL INFRASTRUCTURE AND KEY RESOURCES

Critical infrastructure are the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

Sharing Information with the Private Sector

Mission Stories

Cyber Intelligence Network: Facilitating the Rapid Exchange of Cyber Intelligence

Department of the Interior Establishes Dam Sector Intelligence Working Group

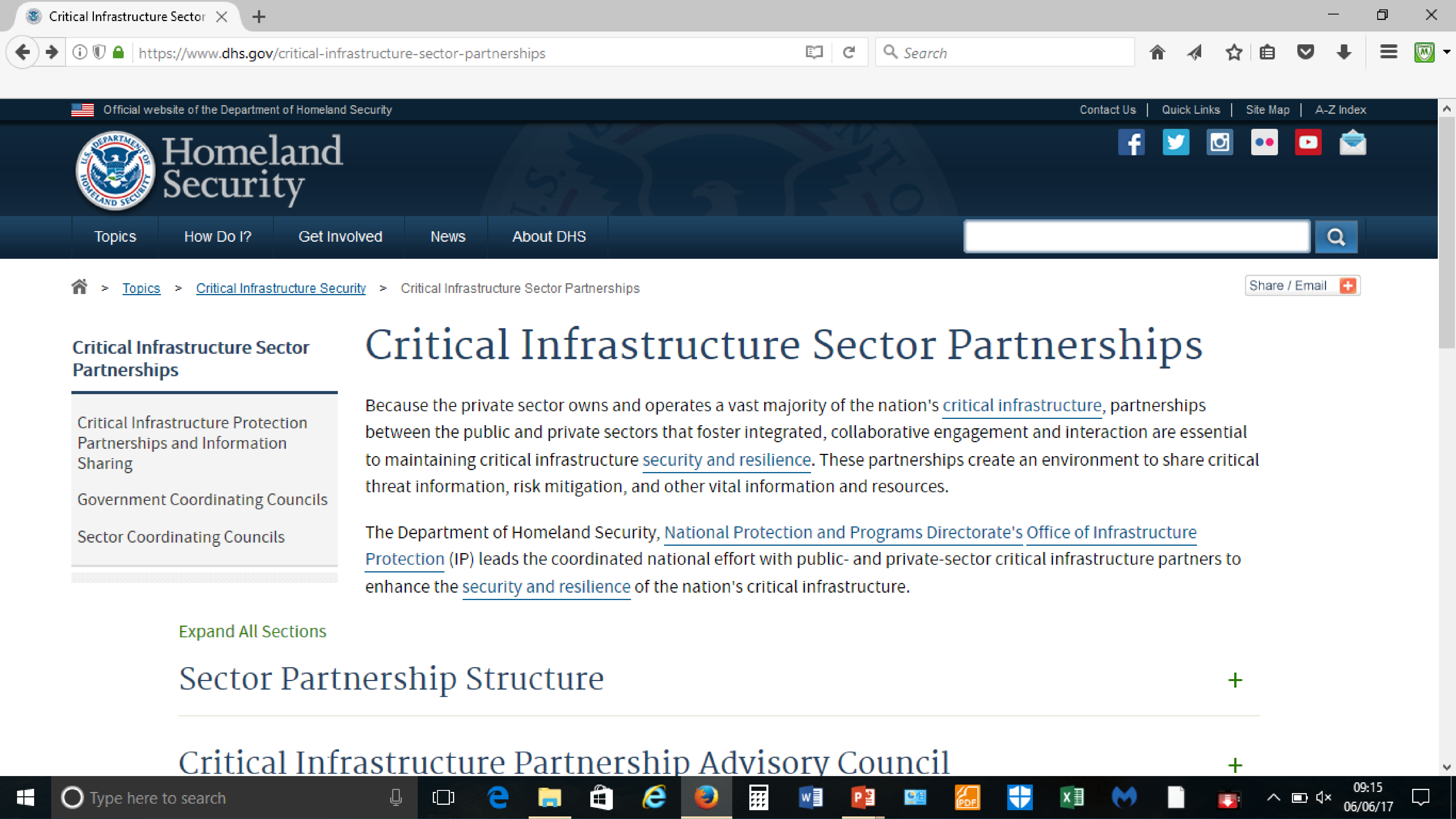
VIEW ALL MISSION STORIES ›

Resources

ISE Core Mission Processes

VIEW ALL RESOURCES ›

Tools


Critical Infrastructure Sector
https://www.dhs.gov/critical-infrastructure-sector-partnerships
Search
Official website of the Department of Homeland Security
Contact Us | Quick Links | Site Map | A-Z Index
Homeland Security
Topics
How Do I?
Get Involved
News
About DHS
Topics > Critical Infrastructure Security > Critical Infrastructure Sector Partnerships
Share / Email
Type here to search
09:15
06/06/17

Critical Infrastructure Sector Partnerships

- Critical Infrastructure Protection Partnerships and Information Sharing
- Government Coordinating Councils
- Sector Coordinating Councils

Critical Infrastructure Sector Partnerships

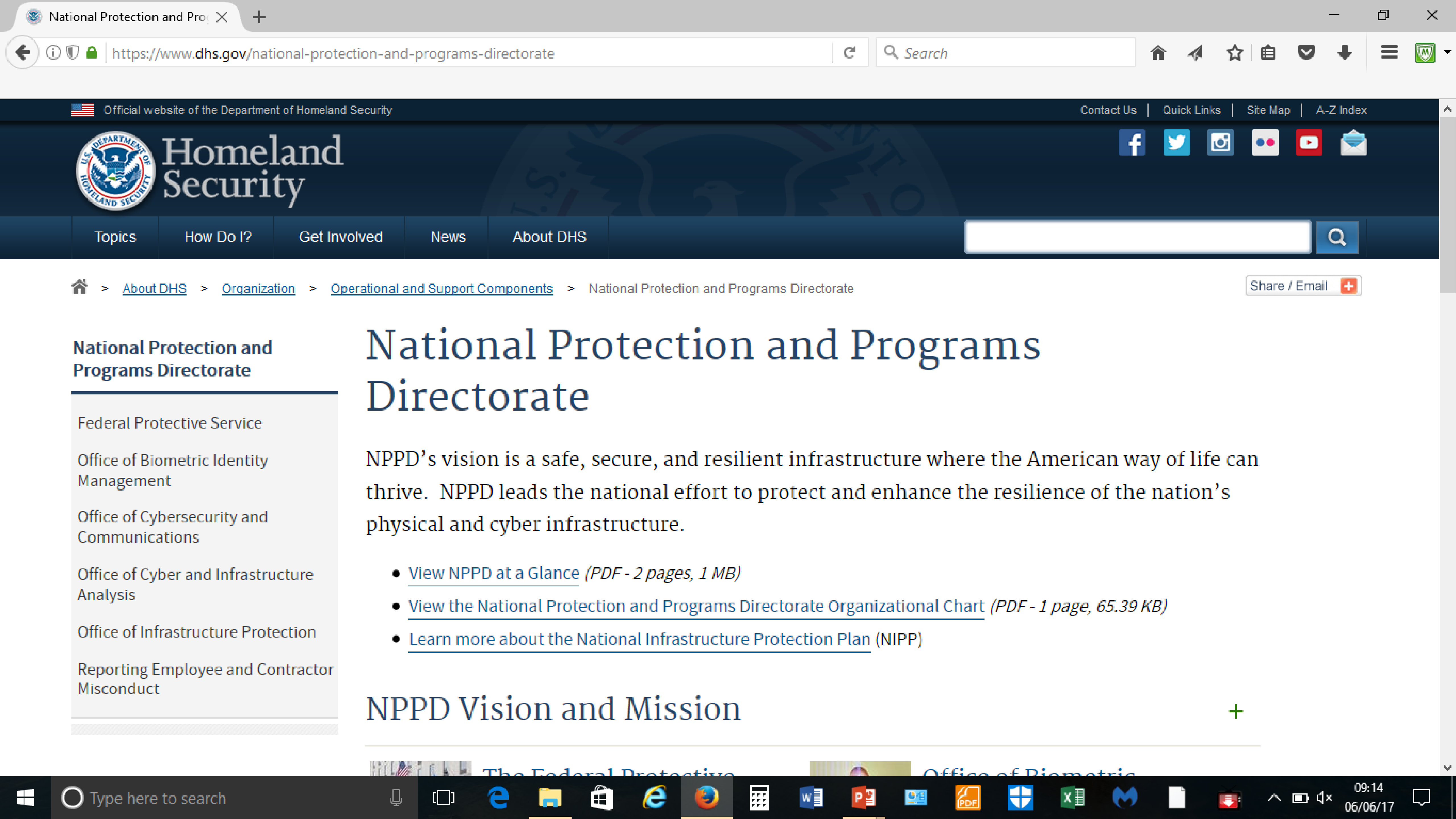
Because the private sector owns and operates a vast majority of the nation's critical infrastructure, partnerships between the public and private sectors that foster integrated, collaborative engagement and interaction are essential to maintaining critical infrastructure security and resilience. These partnerships create an environment to share critical threat information, risk mitigation, and other vital information and resources.

The Department of Homeland Security, National Protection and Programs Directorate's Office of Infrastructure Protection (IP) leads the coordinated national effort with public- and private-sector critical infrastructure partners to enhance the security and resilience of the nation's critical infrastructure.

Expand All Sections

Sector Partnership Structure +

Critical Infrastructure Partnership Advisory Council +


National Protection and Pro
https://www.dhs.gov/national-protection-and-programs-directorate
Search
Official website of the Department of Homeland Security
Contact Us | Quick Links | Site Map | A-Z Index
Homeland Security
Topics
How Do I?
Get Involved
News
About DHS
Share / Email
Type here to search
09:14
06/06/17

About DHS > Organization > Operational and Support Components > National Protection and Programs Directorate

National Protection and Programs Directorate

- Federal Protective Service
- Office of Biometric Identity Management
- Office of Cybersecurity and Communications
- Office of Cyber and Infrastructure Analysis
- Office of Infrastructure Protection
- Reporting Employee and Contractor Misconduct

National Protection and Programs Directorate

NPPD's vision is a safe, secure, and resilient infrastructure where the American way of life can thrive. NPPD leads the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure.

- View NPPD at a Glance *(PDF - 2 pages, 1 MB)*
- View the National Protection and Programs Directorate Organizational Chart *(PDF - 1 page, 65.39 KB)*
- Learn more about the National Infrastructure Protection Plan (NIPP)

NPPD Vision and Mission +

The Federal Protective

Office of Biometric

Vulnerability Checklist - H...
AOL Mail (928)
Critical Infrastructure and ...
https://www.dhs.gov/critical-infrastructure-and-key-resources-support-annex
Search
Official website of the Department of Homeland Security
Contact Us
Quick Links
Site Map
A-Z Index
Homeland Security
Topics
How Do I?
Get Involved
News
About DHS
Share / Email
Search Windows
13:41
11/25/16

About DHS > Organization > Operational and Support Components > National Protection and Programs Directorate > Office of Infrastructure Protection > National Infrastructure Coordinating Center > Critical Infrastructure and Key Resources Support Annex

National Infrastructure Coordinating Center

Critical Infrastructure and Key Resources Support Annex

Critical Infrastructure and Key Resources Support Annex

The Critical Infrastructure and Key Resources (CIKR) Support Annex describes policies, roles and responsibilities, and the concept of operations for assessing, prioritizing, protecting, and restoring critical infrastructure and key resources of the United States and its territories and possessions during actual or potential domestic incidents. The annex details processes to ensure coordination and integration of CIKR-related activities among a wide array of public and private incident managers and CIKR security partners within immediate incident areas as well as at the regional and national levels. Specifically, the annex does the following:

- Describes roles and responsibilities for CIKR preparedness, protection, response, recovery, restoration, and continuity of operations relative to National Response Framework (NRF) coordinating structures and National Incident Management System (NIMS) guiding principles.
- Establishes a concept of operations for incident-related CIKR preparedness, protection, response, recovery, and restoration.
- Outlines incident-related actions (including preresponse and postresponse) to expedite information sharing and analysis of actual or potential impacts to CIKR and facilitate requests for assistance and information from public- and private-sector partners.

Read the Critical Infrastructure and Key Resources Support Annex - *(PDF - 36 pages, 357 KB)*

Last Published Date: August 26, 2015

Terrorism Threat

- Terrorism is defined by the FBI as; “The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.”

Major Terrorism Categories

- International*

- Domestic*

- Single Issue-Special Interest

- Lone wolf/micro-actor/homegrown violent extremist (HVE)

* Defined in US Code Title 18 Section 2331

Special Interest-Single Issue

- **Earth Liberation Front**
- **Animal Liberation Front**
- **Stop Huntingdon Animal Cruelty (SHAC)**
- **Anti-abortion groups**

S.H.A.C. Group

- Targeted both Huntingdon Life Sciences and their suppliers.
- Performed tests on animals.
- S.H.A.C. ceased their activities in 2014.

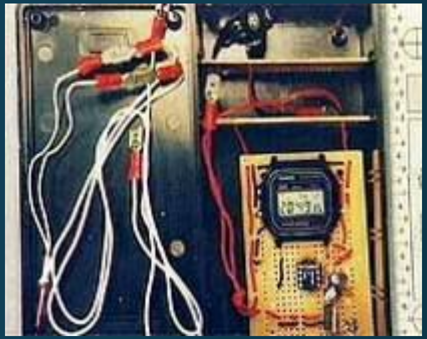
Photo credit:https://en.wikipedia.org/w/index.php?curid=22000454

Potential Attack Targets

- Business
- Government
- Maritime
- Military
- First responders
- Private citizens & property
  - Public venues
  - Schools/Universities
- Religious institutions
- Transportation
- Symbolic

The Hierarchy of the WMD Threat

- Cyber attack
- Explosives
- Biological toxins
- Industrial chemicals
- Biological pathogens
- Radiological isotopes
- Military chemical agents
- Nuclear weapons



Al-Qaeda Business Tactic

- Operation Hemorrhage
  - Inflict heavy economic damage
  - Use low cost operations
  - Smaller, more frequent attacks
  - “Strategy of a thousand cuts”
    - Object is to bleed the enemy to death.

- First successful on September 03, 2010.
  - A UPS cargo plane exploded after takeoff from Dubai International Airport.

Package Bombs

- Addressed to infamous peo
  involved in the Crusades ar
  Spanish Inquisition.
- One of the synagogues allegedly has gay/lesbian members.

NOVEMBER 1431 | 2010
INSPIRE
Al-Malahem Media
OBTAINED BY CNN
The Objectives of Operation Hemorrhage | Technical Details | Exclusive Images

WIRED MailOnline

Hydroelectric Plant IED Attack

- July 21, 2010- Northern Russia
- Perpetrators killed two security guards to gain entry.
  - Detained & assaulted & detained to employees.
- Placed up to five IED’s, four of which detonated.
  - One rendered safe.

Hydroelectric Plant IED Attack

- Two of the plant’s three generators destroyed.
  - Fire took three and a half hours to extinguish.
- Attack at a police station in a nearby town one hour prior may have been distracter/diversion event.

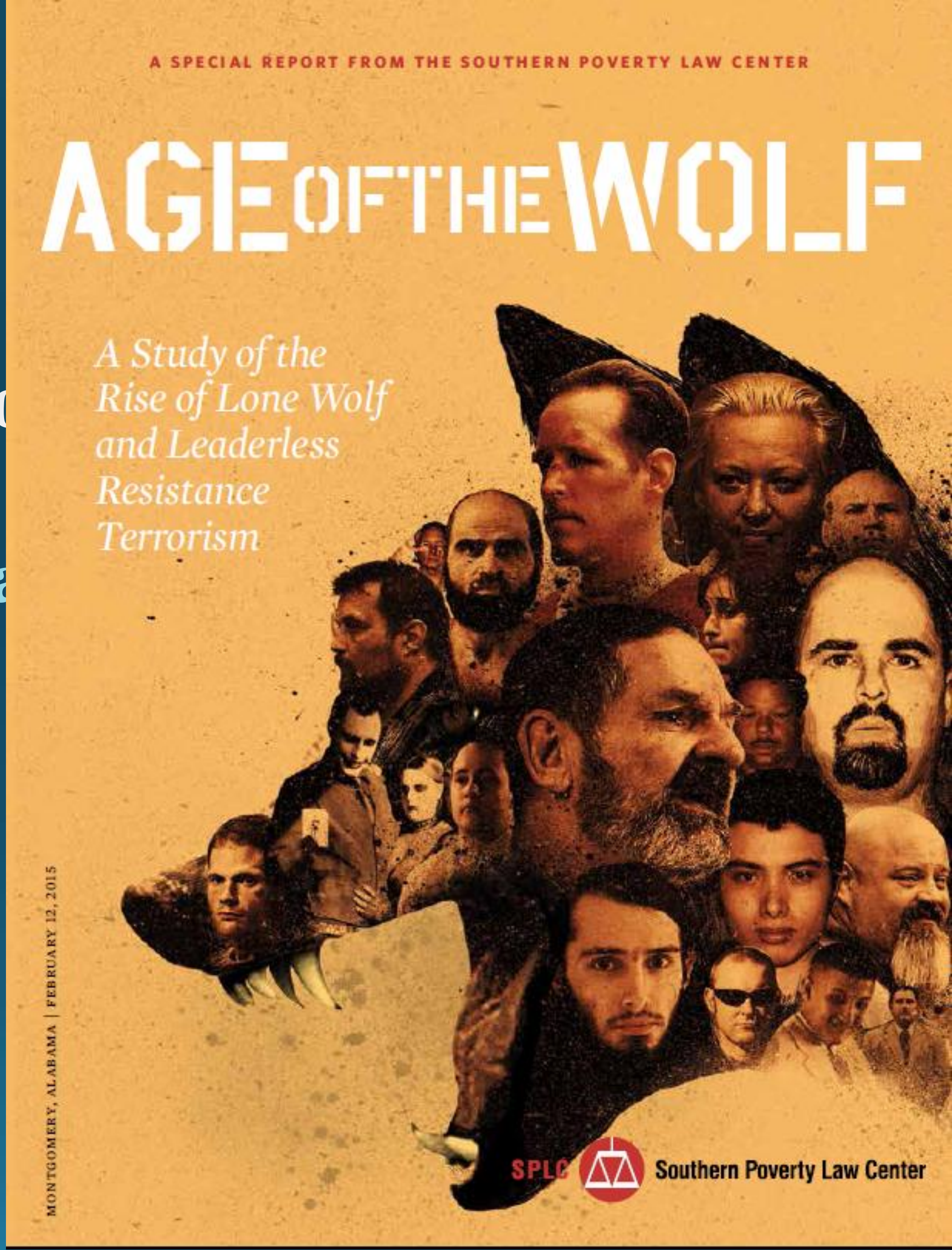
Current Threat

- Due to the proliferation of available radicalization material, the threat has evolved from spectacular events such as the Murrah Building and WTC attacks to smaller events carried out by individuals or smaller groups.
- This type of activity is difficult to track, investigate, and prevent.
- Magazines, books, Internet information contribute to self radicalization.

Current Threat

- “The Age of the Wolf”- Southern Po
  - 44 page document
  - Describes the rise of lone wolf a resistance terrorism

- Aka: HVE
  - Homegrown Violent Extremist



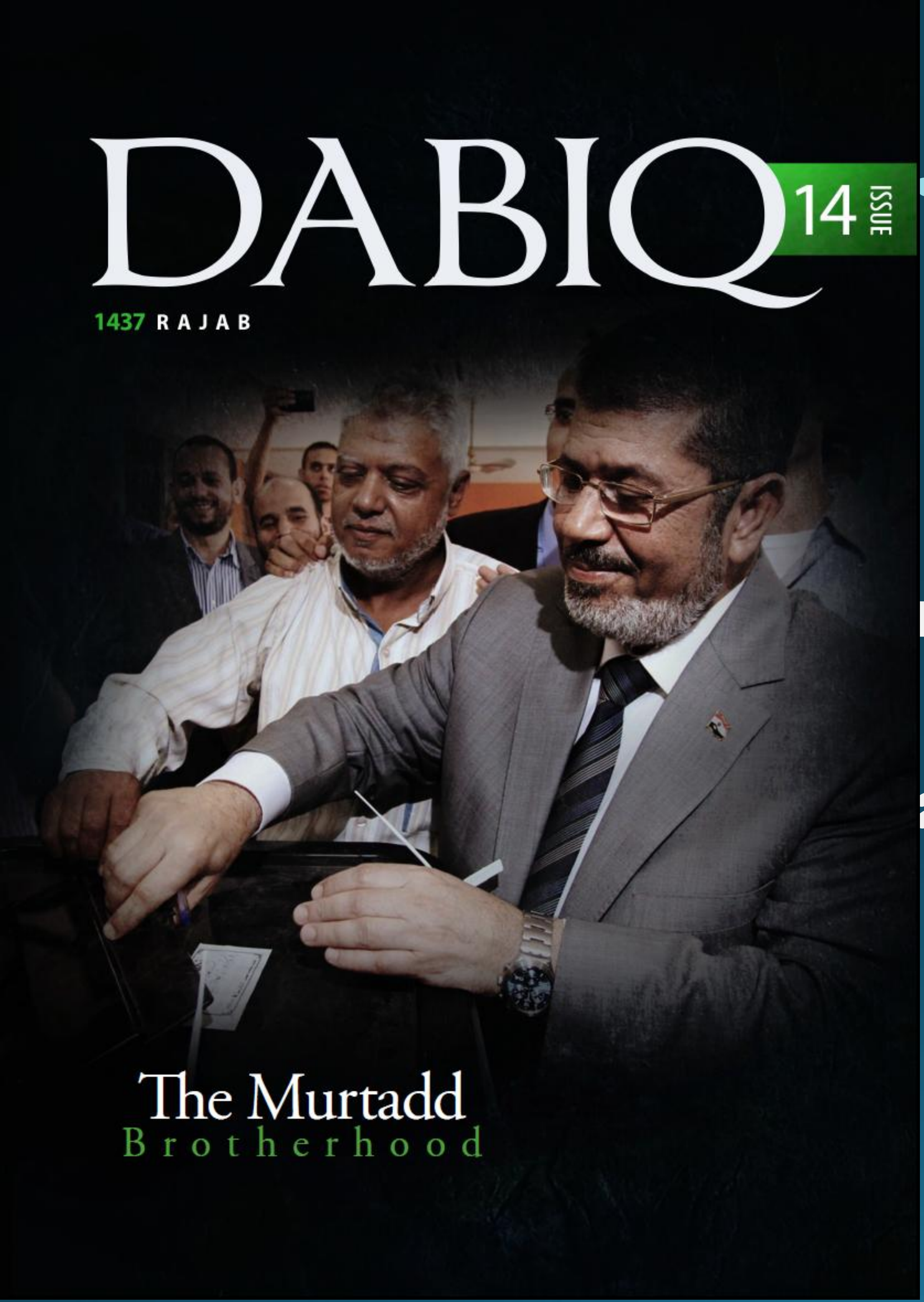
A SPECIAL REPORT FROM THE SOUTHERN POVERTY LAW CENTER

AGE OF THE WOLF

A Study of the Rise of Lone Wolf and Leaderless Resistance Terrorism

MONTGOMERY, ALABAMA | FEBRUARY 12, 2015

SPLC Southern Poverty Law Center



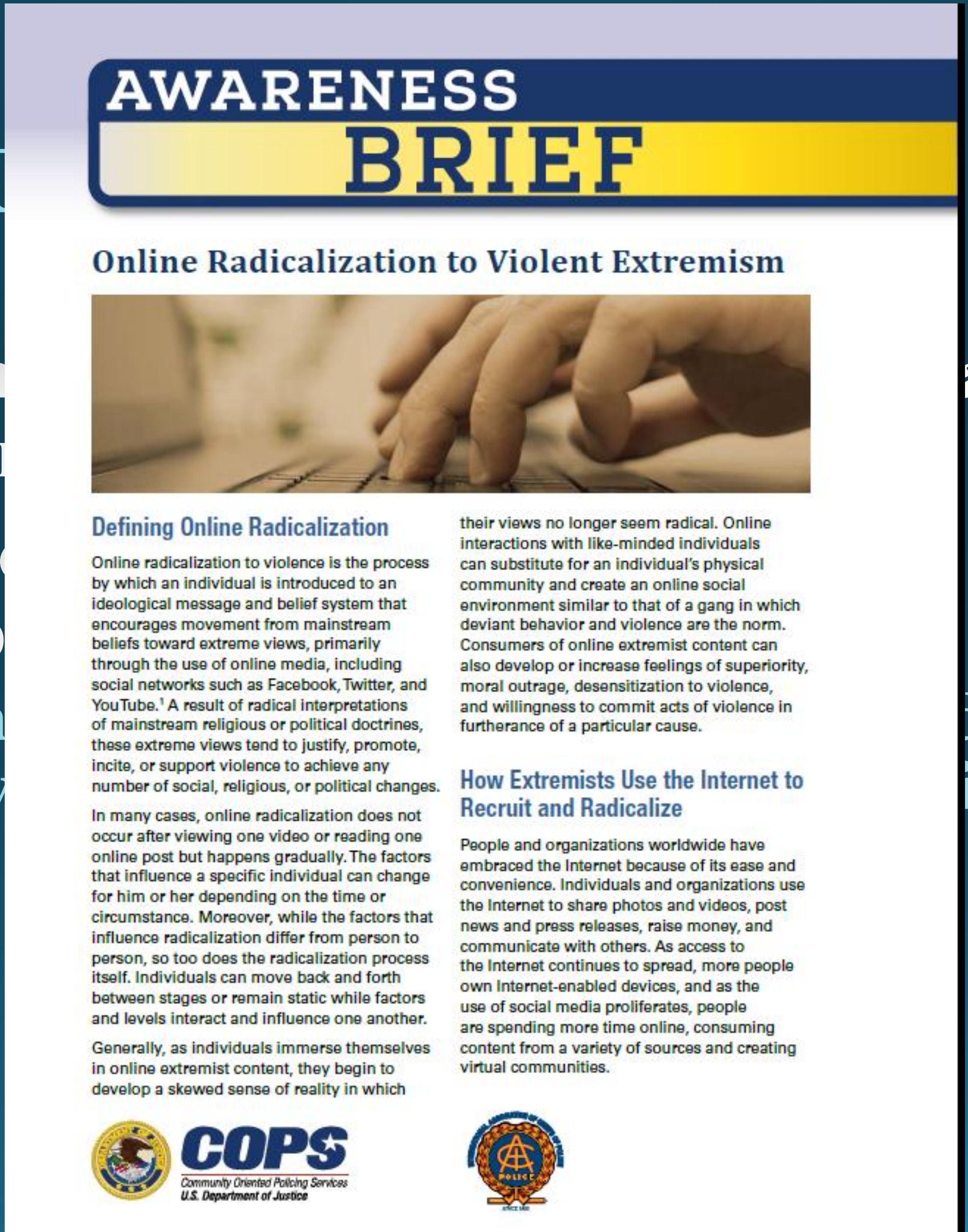
roliferat

material ava

ars now tak

Current T

- U.S. Departm age brief addressing o
- All current s to recruit converts to p
  - Once som directed to more priv ination.



AWARENESS BRIEF

Online Radicalization to Violent Extremism

Defining Online Radicalization

Online radicalization to violence is the process by which an individual is introduced to an ideological message and belief system that encourages movement from mainstream beliefs toward extreme views, primarily through the use of online media, including social networks such as Facebook, Twitter, and YouTube.[1] A result of radical interpretations of mainstream religious or political doctrines, these extreme views tend to justify, promote, incite, or support violence to achieve any number of social, religious, or political changes.

In many cases, online radicalization does not occur after viewing one video or reading one online post but happens gradually. The factors that influence a specific individual can change for him or her depending on the time or circumstance. Moreover, while the factors that influence radicalization differ from person to person, so too does the radicalization process itself. Individuals can move back and forth between stages or remain static while factors and levels interact and influence one another.

Generally, as individuals immerse themselves in online extremist content, they begin to develop a skewed sense of reality in which their views no longer seem radical. Online interactions with like-minded individuals can substitute for an individual's physical community and create an online social environment similar to that of a gang in which deviant behavior and violence are the norm. Consumers of online extremist content can also develop or increase feelings of superiority, moral outrage, desensitization to violence, and willingness to commit acts of violence in furtherance of a particular cause.

How Extremists Use the Internet to Recruit and Radicalize

People and organizations worldwide have embraced the Internet because of its ease and convenience. Individuals and organizations use the Internet to share photos and videos, post news and press releases, raise money, and communicate with others. As access to the Internet continues to spread, more people own Internet-enabled devices, and as the use of social media proliferates, people are spending more time online, consuming content from a variety of sources and creating virtual communities.

COPS
Community Oriented Policing Services
U.S. Department of Justice

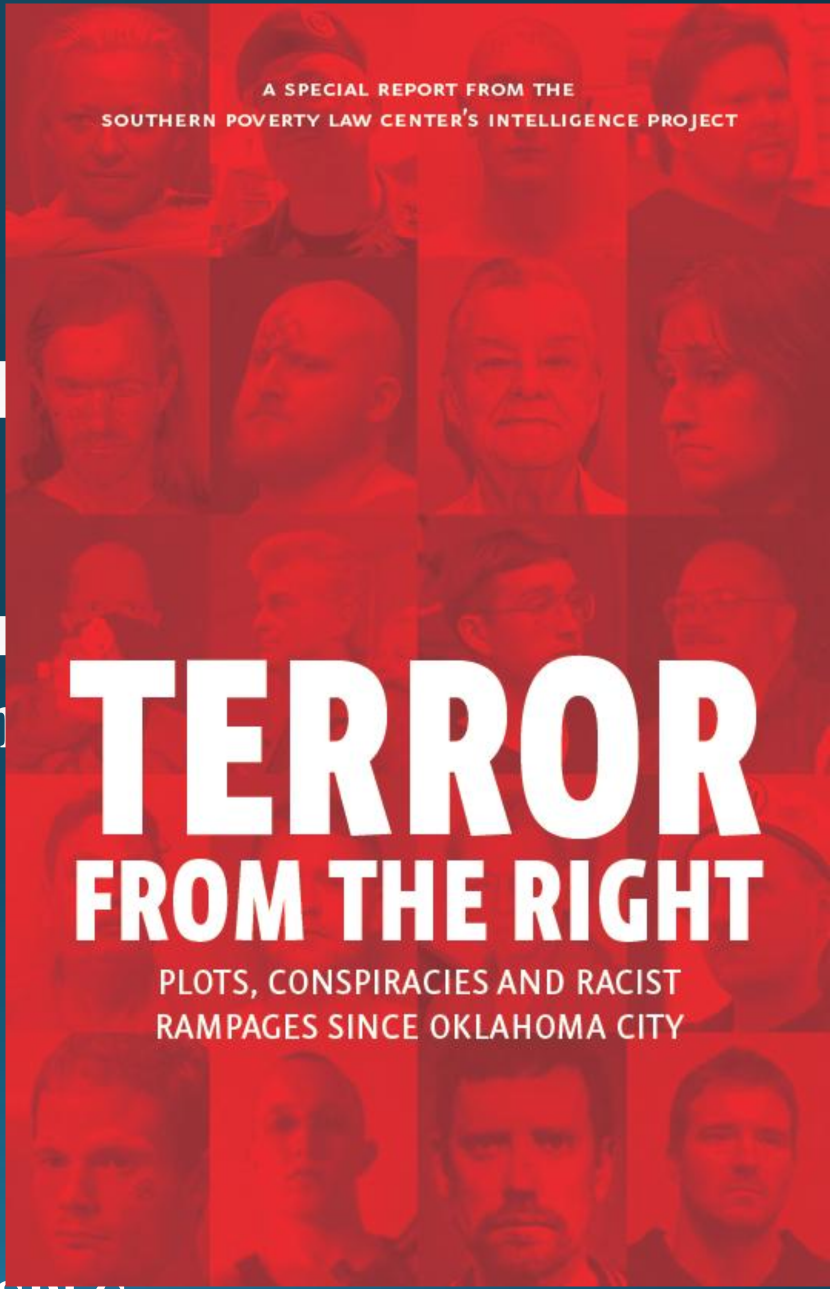
Current Threat

- January 26, 2016
- Milwaukee man arrested aft
  & silencers.
  - Target was a Masonic te
  - Wanted to kill 30 people
- Goal to incite more attacks.
  - "I am telling you, if this
    known all over the worl

Photo credit: Twitter.com

Current Threat

- The "Right Wing" Domestic threat is still
- Nearly 100 plots/actions have occurred ar disrupted the 1995 Murrah Building bom
- Most contemplated deaths of large numb
  - In one case, as many as 30,000.


A SPECIAL REPORT FROM THE
SOUTHERN POVERTY LAW CENTER'S INTELLIGENCE PROJECT
TERROR
FROM THE RIGHT
PLOTS, CONSPIRACIES AND RACIST
RAMPAGES SINCE OKLAHOMA CITY

Source: "Terror from the Right" Special Report, SPLC

Current Threat

- Right Wing plans included bombing:
  - Government buildings
  - Banks
  - Refineries
  - Utilities
  - Clinics
  - Synagogues
  - Mosques
  - Memorials
  - Bridges

Photo credit: http://www.motherjones.com

Photo credit: http://www.bcbridges.org

Infra

- Three ight wing e tanks in Elk
  - Ea ropane.
- Dubb the tank f

http://www.panoramio.com/photo/18929943

Current T

Photo credit:
Sedgwick County
Sheriff's Office via AP

Story credit:
http://www.businessinsider.com/
and AP

- Kansas Militi bing plot disrupted.
- Three men planned to detonate four car bombs at an apartment complex where over 100 Somalis resided and that contained a mosque the day after the 2016 Election.

Population around 27K

Insider Vulnerability

- The insider threat may involve harm to physical facilities, personnel.
- It could also involve non-violent actions, centered round sensitive security information, trade secrets, business continuity plans, etc.
- Ensuring employees are trained to the level of knowledge commensurate with their duties is one method to protect valuable assets.

(U//FOUO) Insider Threats

- **(U//FOUO) Terrorism Insider Threat Indicators: The following indicators of insider threats can reflect criminal activity unrelated to terrorism or legitimate terrorism-related activities.**
  - **The presence of multiple indicators especially in combination with other situational information—should raise concerns about a terrorist insider threat.**

(U) Potential Indicators of the Insider Threat:

- (U) Attempts to gain information from employees on topics outside a questioner's area of responsibility.
- (U) Repeated attempts to enter restricted areas without proper credentials.
- (U) Unauthorized copying of sensitive files—particularly blueprints of buildings or critical systems, such as security and fire suppression systems.
- (U) Threats made by disgruntled employees.

(U) Potential Indicators of the Insider Threat:

- (U) Improper use of information technology systems or repeated attempts to access restricted information.
- (U) Requests for irregular work schedules or attempts to be left alone in a facility.
- (U) Patterns of inaccurate statements or making excuses for irregular behavior.
- (U) Off-duty employees on the property—possibly accompanied by unknown or unauthorized individuals.

Sentenced to 20 years on August 31, 2015 Source: Associated Press/Homeland 1

Insider Attack Averted

- June 8, 201
  - Former
- Wichita ai
  - Van with hoice
- Motivated l vith an individual v ipporting violent jiha

REUTERS

Insider Threat

- British Airways worker faces terror charge.
  - Computer specialist allegedly was plotting suicide bombings.
    - Including one he planned to carry out himself.
- Rajib Karim, 30, Bangladesh native,
  - Deliberately took job to further terrorist conspiracy.
  - Would volunteer to join flight crew if employees strike. (Which they did.)

boston.com

AP Associated Press

BRITISH AIRWAYS

March 12, 2010

Insider Attack

- August 26, 2015
- Two NATO soldiers killed by two men wearing Afghan security force uniforms.
- Third "insider attack" this year.
  - An Army Major was killed by in insider in August of 2014.
  - Highest ranked US Officer to be slain in combat since the Vietnam War in 1970.

http://nypost.com/

Insider Attack

- June 11, 2017
- Afghan soldier opens fire on American troops
  - Second insider attack this year
    - In March, three soldiers were wounded when an Afghan soldier opened fire within the confines of a U.S. Special Operations base in Helmand Province.
- Three killed
- Attacker also killed

Multiple sources: The Washington Post, BBC, ABC News, Aljazeera

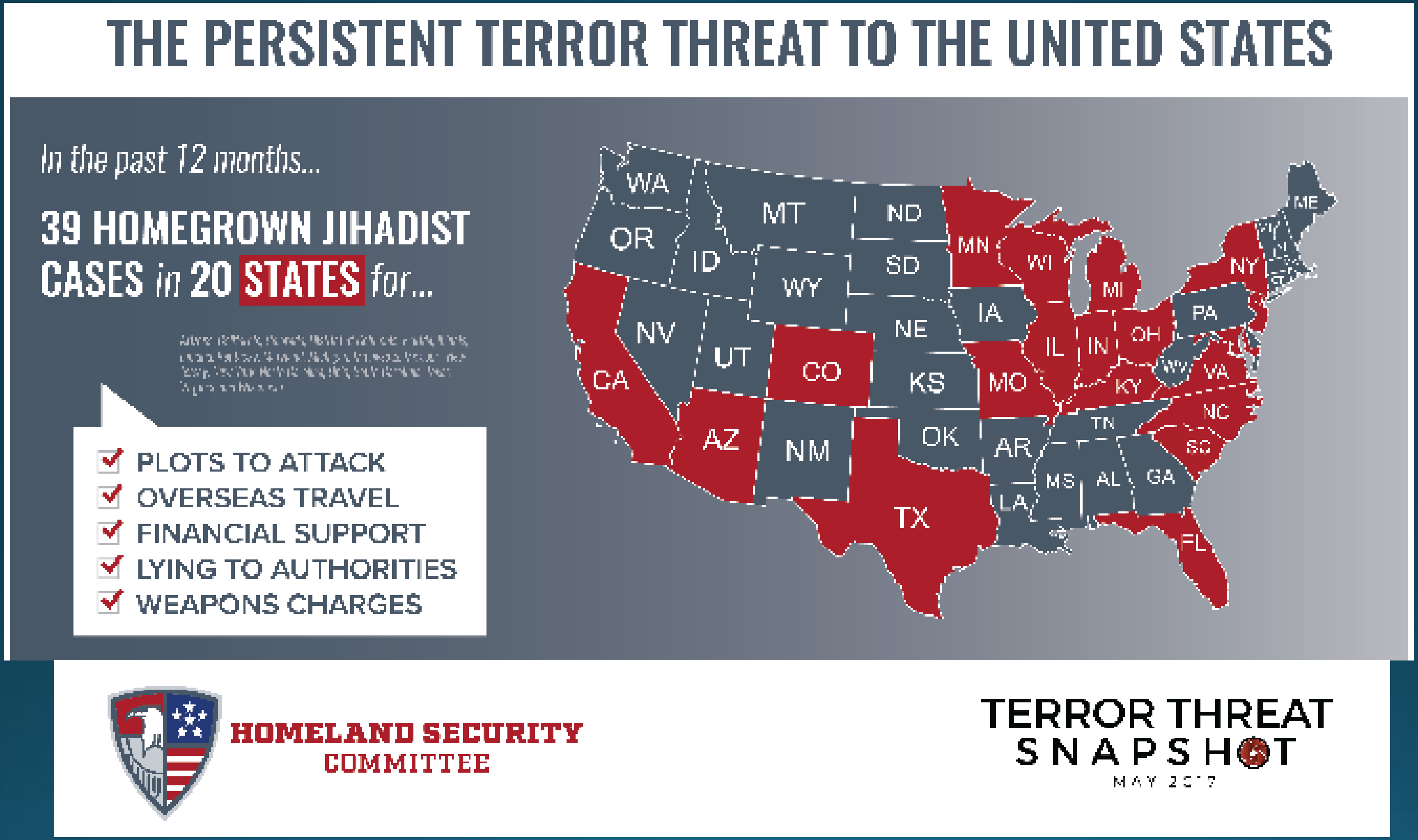
SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Current Threat

- Cyber attacks could compromise infrastructure.

- Targets include:
  - Power grids
  - Wastewater treatment plants
  - Oil/gas pipelines
  - Planes
  - Medical devices

http://www.hospira.com



THE PERSISTENT TERROR THREAT TO THE UNITED STATES

In the past 12 months...

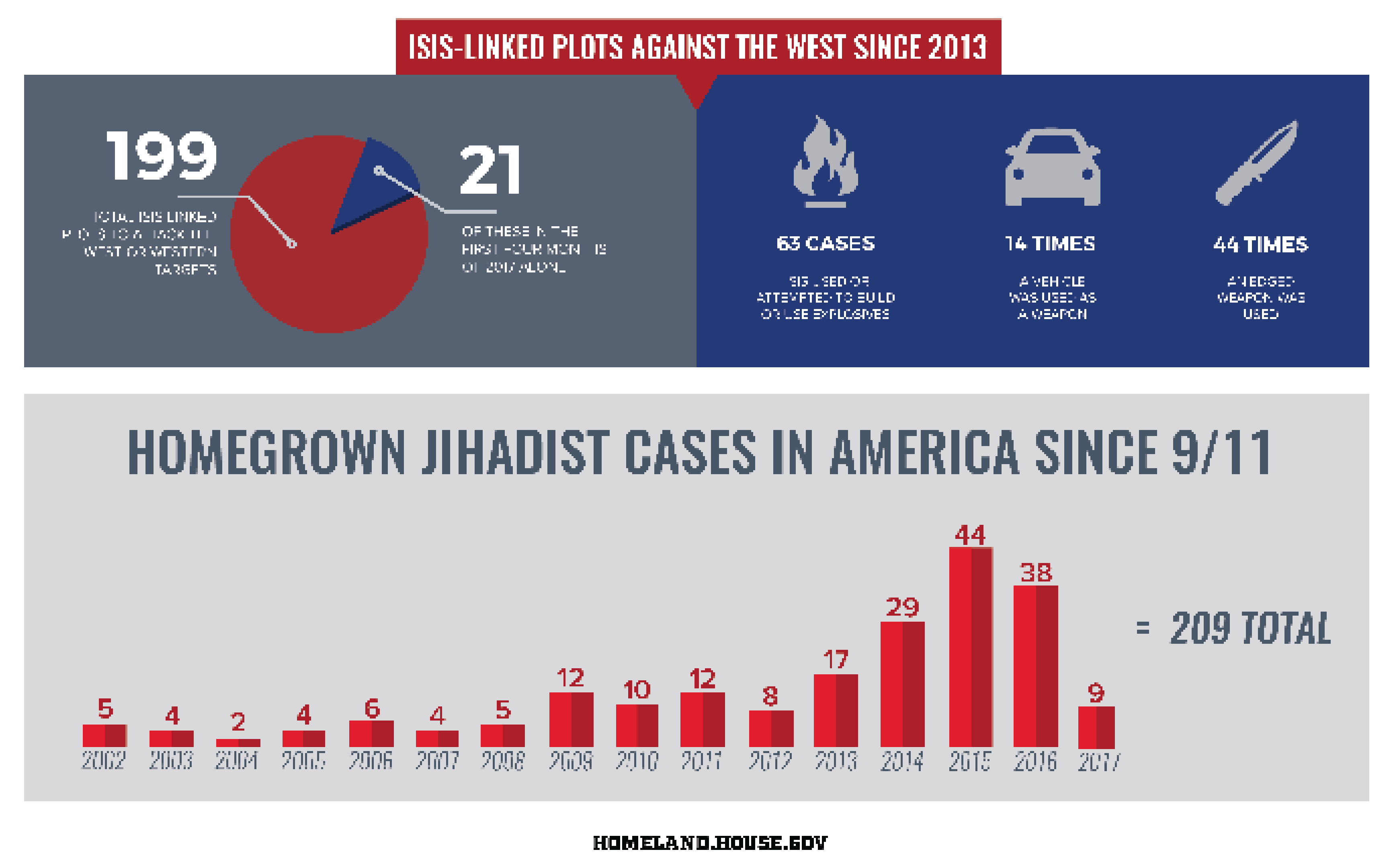
39 HOMEGROWN JIHADIST CASES *in* 20 STATES *for...*

[illegible]

- ☑ PLOTS TO ATTACK
- ☑ OVERSEAS TRAVEL
- ☑ FINANCIAL SUPPORT
- ☑ LYING TO AUTHORITIES
- ☑ WEAPONS CHARGES

HOMELAND SECURITY COMMITTEE

TERROR THREAT SNAPSHOT
MAY 2017



ISIS-LINKED PLOTS AGAINST THE WEST SINCE 2013

HOMEGROWN JIHADIST CASES IN AMERICA SINCE 9/11

HOMELAND.HOUSE.GOV

Religious Dates

- Ramadan, 30 day period of fasting and reflection for Muslims has been called upon by ISIL for its followers to wage “all-out war” on the “infidels” of the West.
- Same request was made in 2016; results:
  - The final global body count after the month-long rampage was 421 dead and 729 wounded.

The Telegraph

Reli

- S
  I

s

- P   Notre
  Dar

Power Grid Cyber Attack

- January 4, 2016-Ukraine
- First known hacker caused power outage perpetrated.
  - December 23, 2015 date of attack.
- Electrical substations disconnected.
  - Hundreds of thousands of homes without electricity.

http://arstechnica.com/

Bank System Cyber Hack

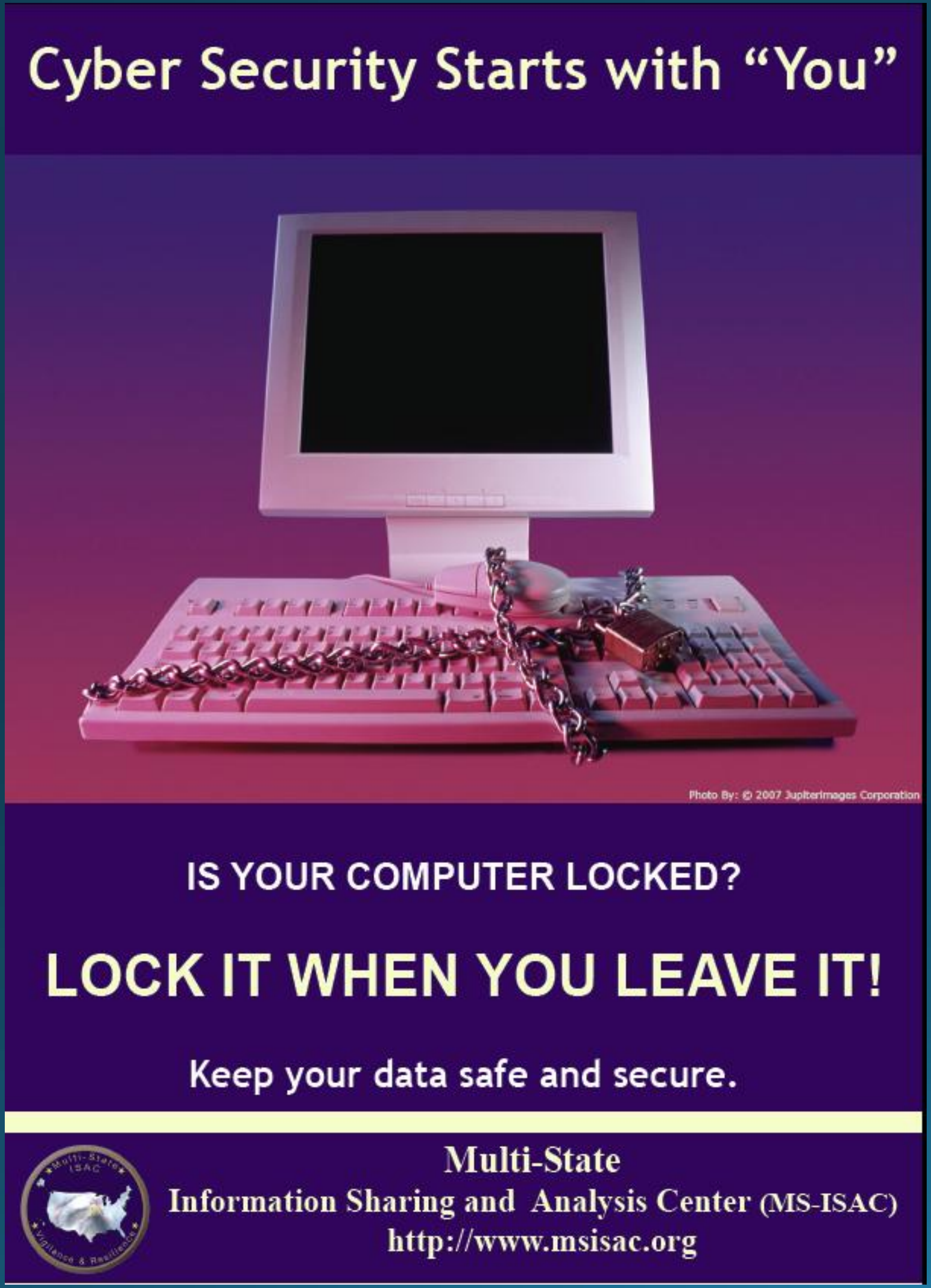
- May 1, 2016
- 81M stolen from Bangladesh's Central Bank.
- Hackers broke into the "Rolls-Royce of payment networks".
  - SWIFT- Society for Worldwide Interbank Financial Telecommunication.
- May 13, 2016 another heist occurred, same system, bank/amount not named.

Current Threat

ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

- Cyberterrorist goals:
  - Destroy, incapacitate, exploit critical infrastructure
  - Threaten national security
  - Cause mass casualties
  - Weaken the U.S. economy
  - Damage public morale/confidence
- May use phishing schemes to generate funds/gather sensitive information.



Cyber Security Starts with "You"

Photo By: © 2007 Jupiterimages Corporation

IS YOUR COMPUTER LOCKED?

LOCK IT WHEN YOU LEAVE IT!

Keep your data safe and secure.

Multi-State
Information Sharing and Analysis Center (MS-ISAC)
http://www.msisac.org

iC^3

IC^3.gov Federal Website for filing formal reports of cyber attacks, & information source.

Cyber Attack

- March 18, 2010
- Omar Ramos-Lopez, 20, fired from auto dealership in Texas.
  - Used a former colleagues password to hack into dealerships website.
  - Caused cars to be disabled, set off car horns, ordered $130,000.00 in GPS equipment.

Cyber Hack

- July 21, 201
- Jeep Cherok
  - Air condi nission, brakes al
  - Car ende
- 471,000 vehi

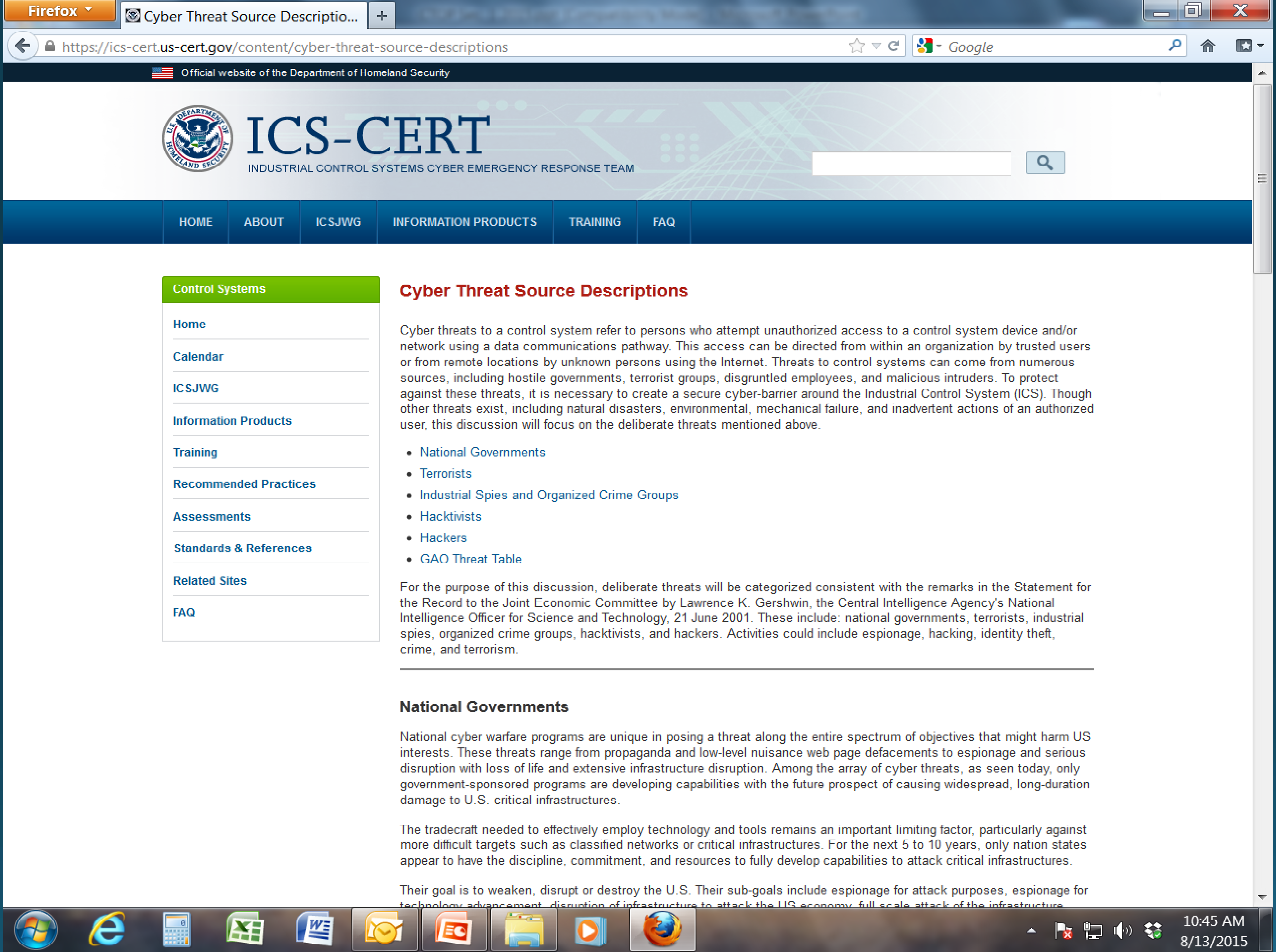
Photo credit:Andy Greenberg/WIRED

http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Energy Sector Cyber Attacks

- Duke Energy
  - Country’s largest electricity Company
  - Manages three of the 16 types of infrastructure critical to human life
- Computer system under constant attack
  - A dozen times in the last decade foreign hackers have gained enough remote access to control the operations networks that keep the lights on.

Sources: The Associated Press & The News&Observer



Cyber Threat Source Descriptions

Cyber threats to a control system refer to persons who attempt unauthorized access to a control system device and/or network using a data communications pathway. This access can be directed from within an organization by trusted users or from remote locations by unknown persons using the Internet. Threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and malicious intruders. To protect against these threats, it is necessary to create a secure cyber-barrier around the Industrial Control System (ICS). Though other threats exist, including natural disasters, environmental, mechanical failure, and inadvertent actions of an authorized user, this discussion will focus on the deliberate threats mentioned above.

- National Governments
- Terrorists
- Industrial Spies and Organized Crime Groups
- Hacktivists
- Hackers
- GAO Threat Table

For the purpose of this discussion, deliberate threats will be categorized consistent with the remarks in the Statement for the Record to the Joint Economic Committee by Lawrence K. Gershwin, the Central Intelligence Agency's National Intelligence Officer for Science and Technology, 21 June 2001. These include: national governments, terrorists, industrial spies, organized crime groups, hacktivists, and hackers. Activities could include espionage, hacking, identity theft, crime, and terrorism.

National Governments

National cyber warfare programs are unique in posing a threat along the entire spectrum of objectives that might harm US interests. These threats range from propaganda and low-level nuisance web page defacements to espionage and serious disruption with loss of life and extensive infrastructure disruption. Among the array of cyber threats, as seen today, only government-sponsored programs are developing capabilities with the future prospect of causing widespread, long-duration damage to U.S. critical infrastructures.

The tradecraft needed to effectively employ technology and tools remains an important limiting factor, particularly against more difficult targets such as classified networks or critical infrastructures. For the next 5 to 10 years, only nation states appear to have the discipline, commitment, and resources to fully develop capabilities to attack critical infrastructures.

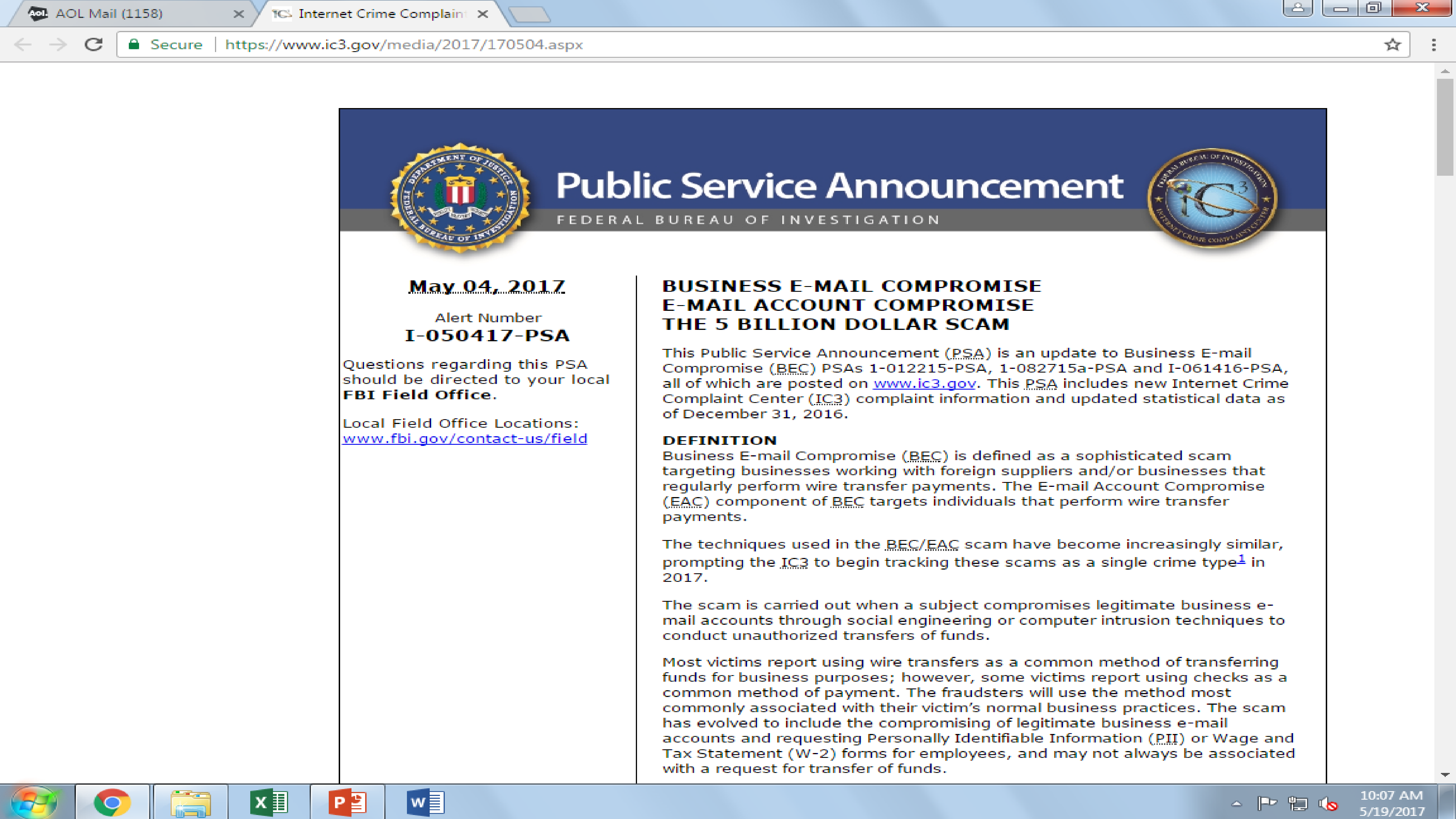
Their goal is to weaken, disrupt or destroy the U.S. Their sub-goals include espionage for attack purposes, espionage for technology advancement, disruption of infrastructure to attack the US economy, full scale attack of the infrastructure

Another Cyber Twist

HOMELAND SECURITY TODAY.US

11.23.16

- Malware covertly turns PCs into eavesdropping devices.
- Headphones, earphones, and speakers can be reprogrammed from output to input.
- Countermeasures include:
  - Completely disabling audio hardware,
  - Using an HD audio driver to alert when microphones are being accessed,
  - Establishing a strict rejacking policy within the industry.



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

May 04, 2017

Alert Number
I-050417-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

BUSINESS E-MAIL COMPROMISE
E-MAIL ACCOUNT COMPROMISE
THE 5 BILLION DOLLAR SCAM

This Public Service Announcement (PSA) is an update to Business E-mail Compromise (BEC) PSAs 1-012215-PSA, 1-082715a-PSA and I-061416-PSA, all of which are posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center (IC3) complaint information and updated statistical data as of December 31, 2016.

DEFINITION

Business E-mail Compromise (BEC) is defined as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The E-mail Account Compromise (EAC) component of BEC targets individuals that perform wire transfer payments.

The techniques used in the BEC/EAC scam have become increasingly similar, prompting the IC3 to begin tracking these scams as a single crime type[1] in 2017.

The scam is carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

Most victims report using wire transfers as a common method of transferring funds for business purposes; however, some victims report using checks as a common method of payment. The fraudsters will use the method most commonly associated with their victim's normal business practices. The scam has evolved to include the compromising of legitimate business e-mail accounts and requesting Personally Identifiable Information (PII) or Wage and Tax Statement (W-2) forms for employees, and may not always be associated with a request for transfer of funds.

International Cyber Hack

- May 12, 2017- 0324 hours
- WannaCry ransomware attack
- 150 countries, >200,000 people victimized as of 05.17.17
  - 40 hospitals in UK affected
- National Security Agency developed tool dumped on line by a group calling itself the Shadow Brokers

Source: USA TODAY TALKING TECH

International Cyber Hack

- “Kill switch” found by a 22 year old British self taught computer worker
  - Other variations observed on May 14
- Microsoft issued patch for vulnerability on March 14, 2017
- Prevention: Install/allow patches for installed software

Current Threat Summary

- Domestic and international actors still pose a real threat to perpetrate an attack within the U.S.
- On-line radicalization of singular individuals/small groups are difficult to identify & track.
  - Teenagers, young children, females, and families are now more prevalent in terrorism activities.
- Continued publication of terror-based magazines provides motivation and direction for home grown violent extremists (HVE).

Current Threat Summary

- There were 1,441 attacks worldwide in 2016, causing 14,356 fatalities*.
- Attacks that are well planned involve target selection, surveillance, practice runs, and possibly testing security measures.
- Employers/employees should take note of and report through established procedures, any activity that may fit into any phase of attack planning.

*Source: https://storymaps.esri.com/stories/terrorist-attacks/?year=2016

Tactical Actions

- Although too numerous to describe in total during this session’s time frame, several actual events are described throughout the rest of the Program.
- The Counter-Terrorism discipline is ever evolving; as we do better at prevention, those who would cause harm explore ways to circumvent our efforts.
- Constant vigilance, situational awareness, and communication are three methods of protection businesses can employ to deter an attack.

Tactical Actions

- January, 2015
- 80% (140 million people) of Pakistan blacked out due to a terrorist bombing of the power grid.
    - Two transmission sites hit.
    - Two nuclear plants also knocked offline.
- Perpetrators may have found a critical focal point of the system.

US Tac

- San Jose
- 17 transf rounds.
  - Attem ure.
- 911 fiber
- Perpetra

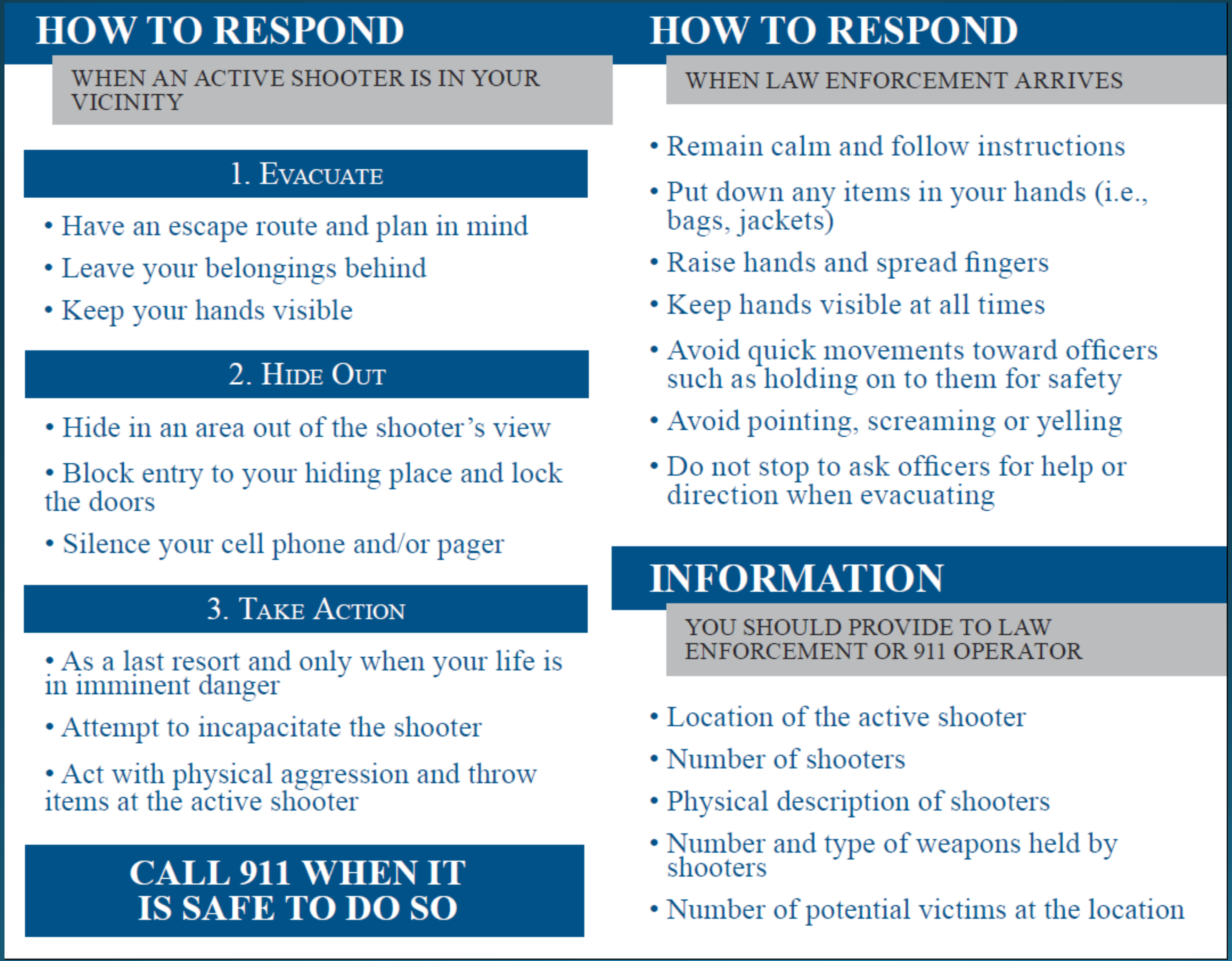
Photo credit: Jim Wilson, NY Times

Source: http://www.wnd.com/

Armed Assault Tactic

- From sharp edged items through and including multiple types of explosives and firearms, the armed assault has become a tool in the terrorist toolbox.
- There is information available for preparation and response to such an event.

On Scene Active Shooter Actions



HOW TO RESPOND

WHEN AN ACTIVE SHOOTER IS IN YOUR VICINITY

1. Evacuate

- Have an escape route and plan in mind
- Leave your belongings behind
- Keep your hands visible

2. Hide Out

- Hide in an area out of the shooter's view
- Block entry to your hiding place and lock the doors
- Silence your cell phone and/or pager

3. Take Action

- As a last resort and only when your life is in imminent danger
- Attempt to incapacitate the shooter
- Act with physical aggression and throw items at the active shooter

CALL 911 WHEN IT IS SAFE TO DO SO

HOW TO RESPOND

WHEN LAW ENFORCEMENT ARRIVES

- Remain calm and follow instructions
- Put down any items in your hands (i.e., bags, jackets)
- Raise hands and spread fingers
- Keep hands visible at all times
- Avoid quick movements toward officers such as holding on to them for safety
- Avoid pointing, screaming or yelling
- Do not stop to ask officers for help or direction when evacuating

INFORMATION

YOU SHOULD PROVIDE TO LAW ENFORCEMENT OR 911 OPERATOR

- Location of the active shooter
- Number of shooters
- Physical description of shooters
- Number and type of weapons held by shooters
- Number of potential victims at the location

On Scene ons

COPIN

WITH AN

- Be awa possible
- Take no facility
- If you a secure t
- Attemp as a last

ing or ed and he use

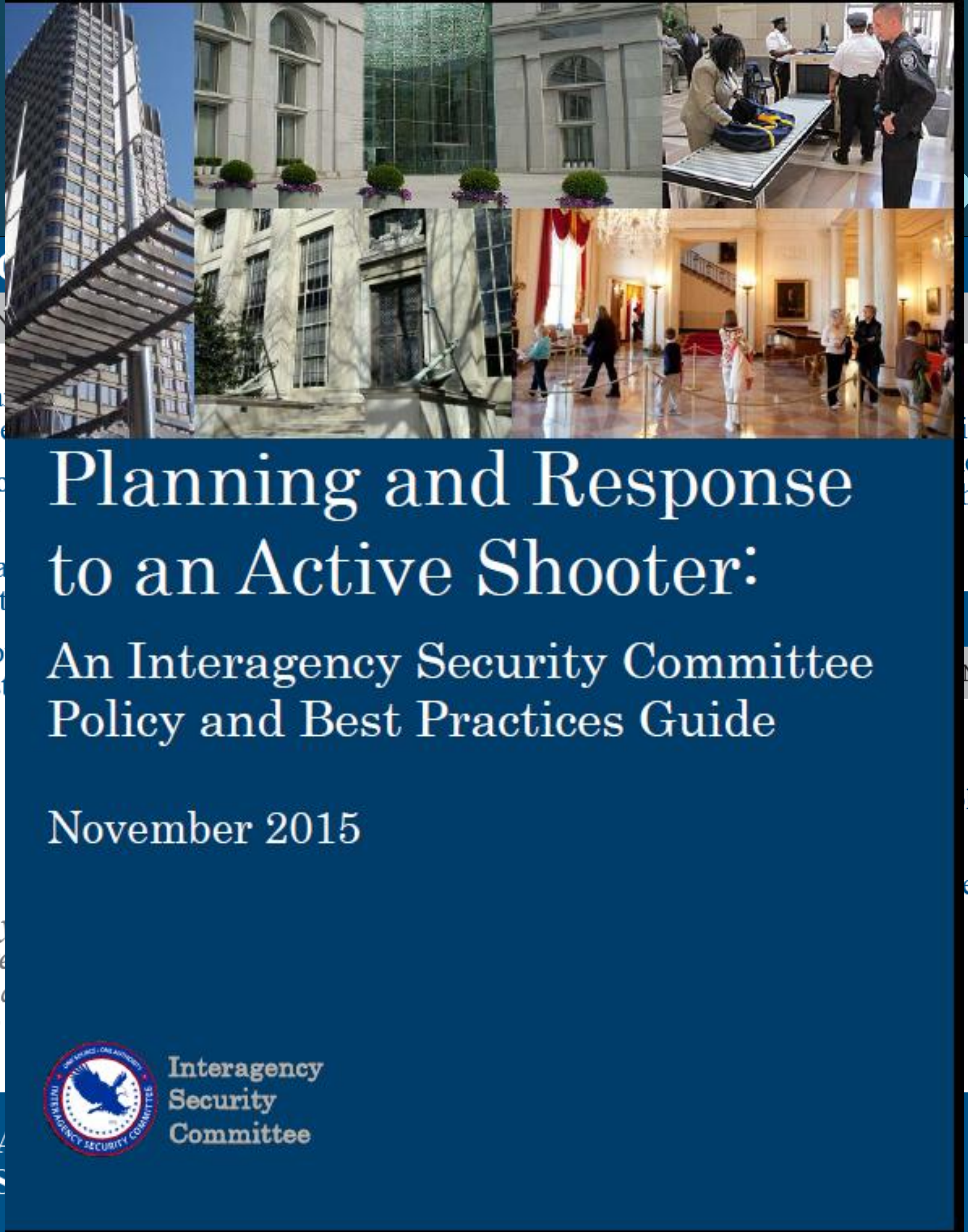
N

lves

ed to

Contact y human re informa shooter

CA IS



Planning and Response to an Active Shooter:

An Interagency Security Committee Policy and Best Practices Guide

November 2015

Interagency Security Committee

When law enforcement arrives:

- Remain calm and follow instructions
- Drop items in your hands (e.g., bags, jackets)
- Raise hands and spread fingers
- Keep hands visible at all times
- Avoid quick movements toward officers, such as holding on to them for safety
- Avoid pointing, screaming or yelling
- Do not ask questions when evacuating

Information to provide to 911 operations:

- Location of the active shooter
- Number of shooters
- Physical description of shooters
- Number and type of weapons shooter has
- Number of potential victims at location

For questions or additional assistance contact:

Your local law enforcement authorities or FBI Field office :

Department of Homeland Security
3801 Nebraska Ave, NW
Washington, DC 20528

ACTIVE SHOOTER EVENTS

When an Active Shooter is in your vicinity, you must be prepared both mentally and physically to deal with the situation.

You have three options:

1 RUN

- Have an escape route and plan in mind
- Leave your belongings behind
- Evacuate regardless of whether others agree to follow
- Help others escape, if possible
- Do not attempt to move the wounded
- Prevent others from entering an area where the active shooter may be
- Keep your hands visible
- Call 911 when you are safe

2 HIDE

- Hide in an area out of the shooter’s view
- Lock door or block entry to your hiding place
- Silence your cell phone (including vibrate mode) and remain quiet

3 FIGHT

- Fight as a last resort and only when your life is in imminent danger
- Attempt to incapacitate the shooter
- Act with as much physical aggression as possible
- Improvise weapons or throw items at the active shooter
- Commit to your actions . . . your life depends on it

The first officers to arrive on scene will not stop to help the injured. Expect rescue teams to follow initial officers. These rescue teams will treat and remove injured.

Once you have reached a safe location, you will likely be held in that area by law enforcement until the situation is under control, and all witnesses have been identified and questioned. Do not leave the area until law enforcement authorities have instructed you to do so.

Vulnerability & Risk Assessment

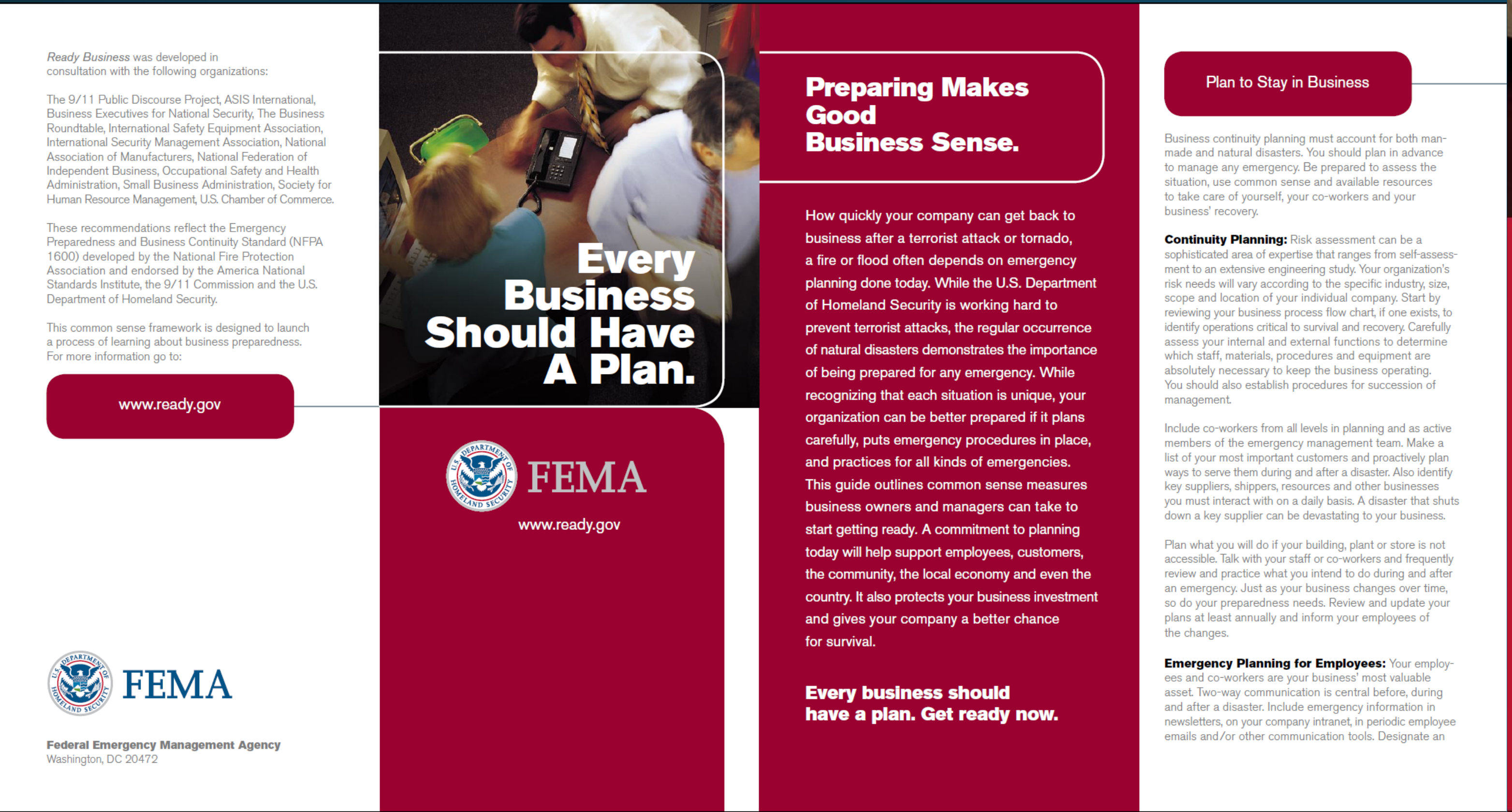
- There is much information available to businesses in assessing their risk and determining the most cost effective solutions to mitigate that risk.
- This next Program segment explores some of those resources.

Risk
Threat
Asset
Vulnerability

HITS HIGH IMPACT TRAINING SOLUTIONS®

Let’s Start with FEMA

- https://www.ready.gov/business
- Quadfold Brochure and 12 page Booklet



Ready Business was developed in consultation with the following organizations:

The 9/11 Public Discourse Project, ASIS International, Business Executives for National Security, The Business Roundtable, International Safety Equipment Association, International Security Management Association, National Association of Manufacturers, National Federation of Independent Business, Occupational Safety and Health Administration, Small Business Administration, Society for Human Resource Management, U.S. Chamber of Commerce.

These recommendations reflect the Emergency Preparedness and Business Continuity Standard (NFPA 1600) developed by the National Fire Protection Association and endorsed by the America National Standards Institute, the 9/11 Commission and the U.S. Department of Homeland Security.

This common sense framework is designed to launch a process of learning about business preparedness. For more information go to:

www.ready.gov

FEMA

Federal Emergency Management Agency
Washington, DC 20472

Every Business Should Have A Plan.

FEMA

www.ready.gov

Preparing Makes Good Business Sense.

How quickly your company can get back to business after a terrorist attack or tornado, a fire or flood often depends on emergency planning done today. While the U.S. Department of Homeland Security is working hard to prevent terrorist attacks, the regular occurrence of natural disasters demonstrates the importance of being prepared for any emergency. While recognizing that each situation is unique, your organization can be better prepared if it plans carefully, puts emergency procedures in place, and practices for all kinds of emergencies. This guide outlines common sense measures business owners and managers can take to start getting ready. A commitment to planning today will help support employees, customers, the community, the local economy and even the country. It also protects your business investment and gives your company a better chance for survival.

Every business should have a plan. Get ready now.

Plan to Stay in Business

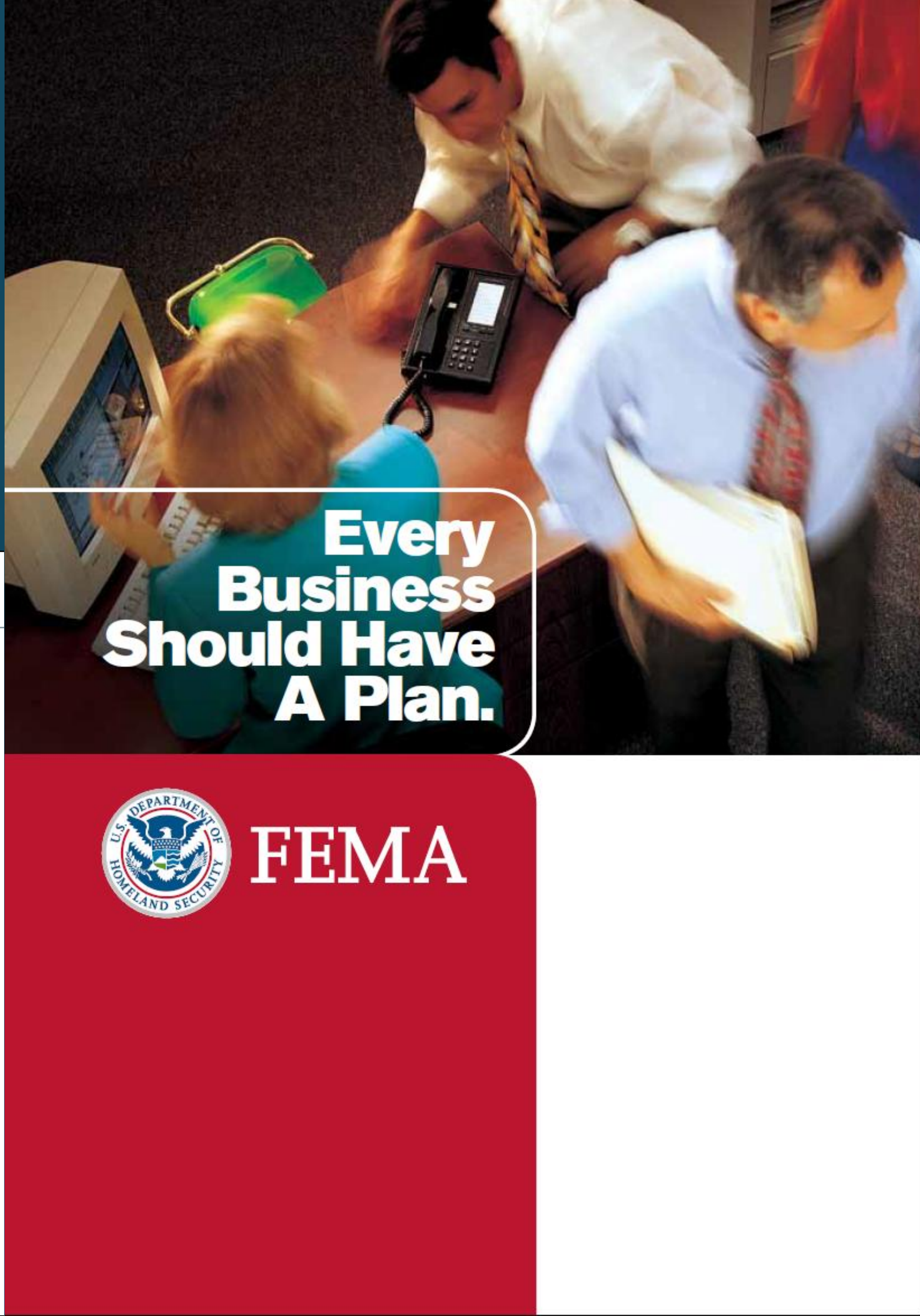
Business continuity planning must account for both man-made and natural disasters. You should plan in advance to manage any emergency. Be prepared to assess the situation, use common sense and available resources to take care of yourself, your co-workers and your business’ recovery.

Continuity Planning: Risk assessment can be a sophisticated area of expertise that ranges from self-assessment to an extensive engineering study. Your organization’s risk needs will vary according to the specific industry, size, scope and location of your individual company. Start by reviewing your business process flow chart, if one exists, to identify operations critical to survival and recovery. Carefully assess your internal and external functions to determine which staff, materials, procedures and equipment are absolutely necessary to keep the business operating. You should also establish procedures for succession of management.

Include co-workers from all levels in planning and as active members of the emergency management team. Make a list of your most important customers and proactively plan ways to serve them during and after a disaster. Also identify key suppliers, shippers, resources and other businesses you must interact with on a daily basis. A disaster that shuts down a key supplier can be devastating to your business.

Plan what you will do if your building, plant or store is not accessible. Talk with your staff or co-workers and frequently review and practice what you intend to do during and after an emergency. Just as your business changes over time, so do your preparedness needs. Review and update your plans at least annually and inform your employees of the changes.

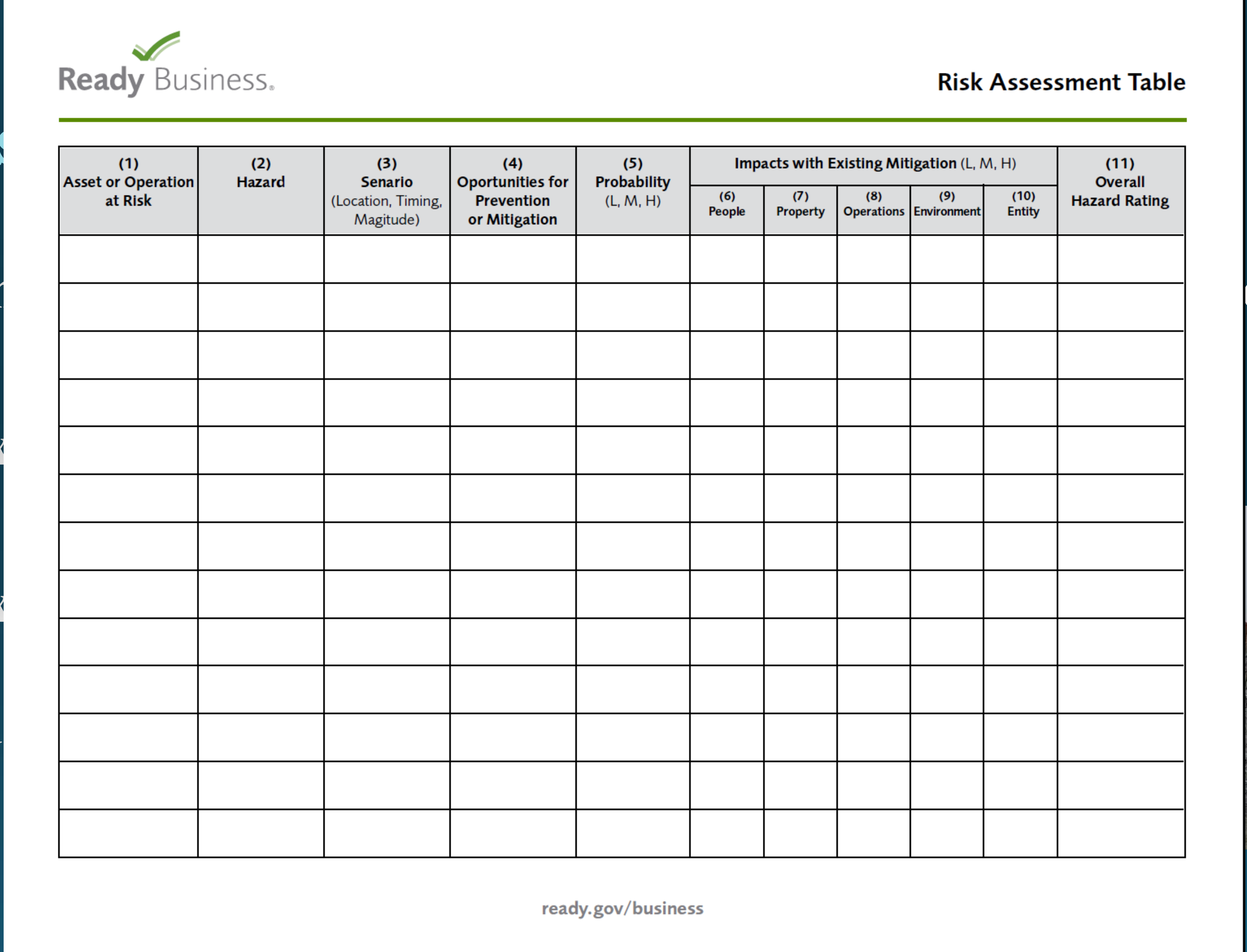
Emergency Planning for Employees: Your employees and co-workers are your business’ most valuable asset. Two-way communication is central before, during and after a disaster. Include emergency information in newsletters, on your company intranet, in periodic employee emails and/or other communication tools. Designate an



Every Business Should Have A Plan.

FEMA

Ris



Ready Business.

Risk Assessment Table

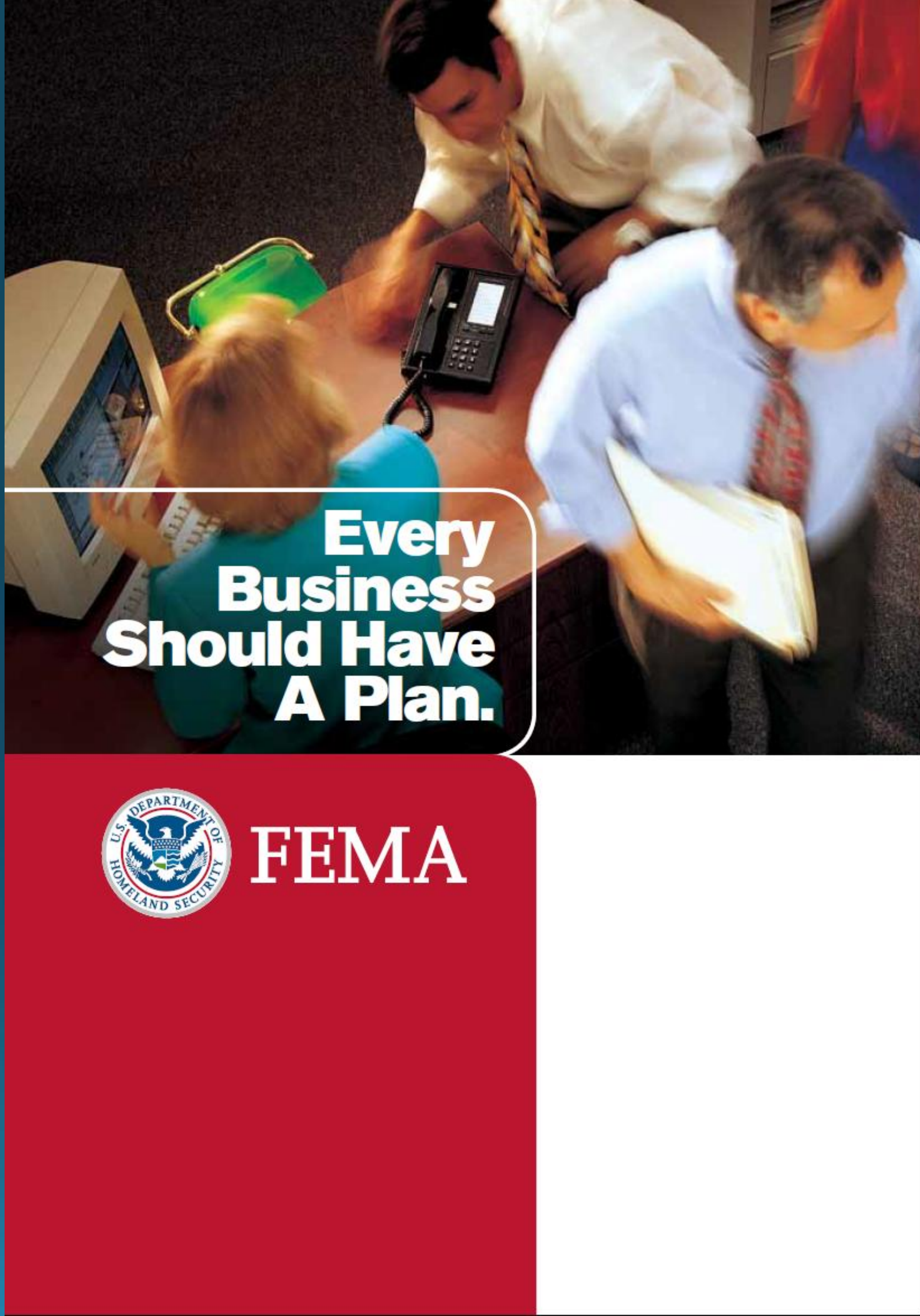
(1) Asset or Operation at Risk	(2) Hazard	(3) Senario (Location, Timing, Magitude)	(4) Oportunities for Prevention or Mitigation	(5) Probability (L, M, H)	Impacts with Existing Mitigation (L, M, H)					(11) Overall Hazard Rating
					(6) People	(7) Property	(8) Operations	(9) Environment	(10) Entity	

ready.gov/business

- Ar ea.
- Ex
- Ex
- W

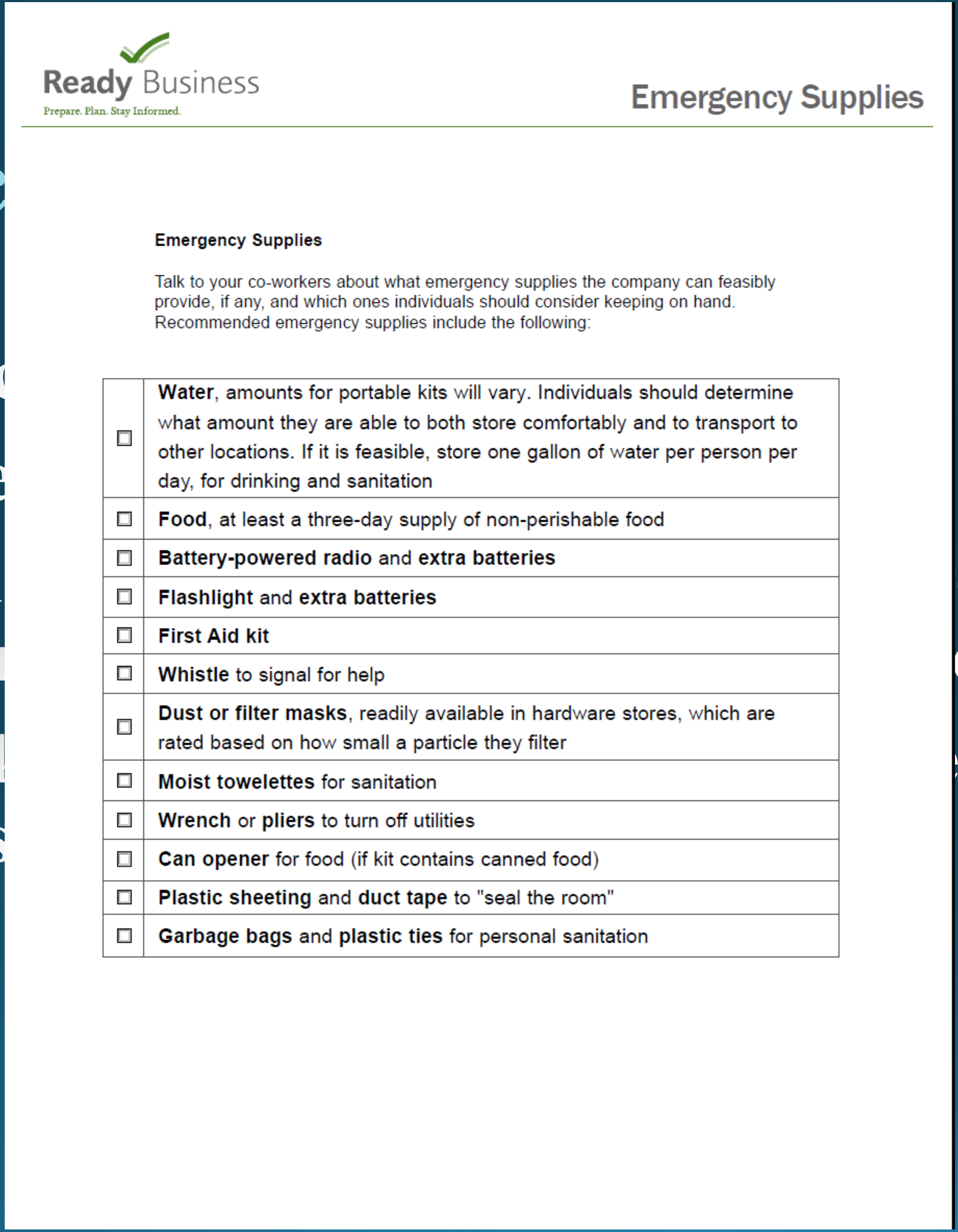
Business Booklet

- 24 point document to assist with preparation, planning, response and recovery for both acts of nature and deliberate events.
- Addresses the all hazards concept.


Every Business Should Have A Plan.
U.S. DEPARTMENT OF HOMELAND SECURITY
FEMA

Emergenc

- Shelter in plac
- No notice eme
- Quickly devel equire your employees to r od of time.
- Using the Risl what level of preparation is



Ready Business
Prepare. Plan. Stay Informed.

Emergency Supplies

Emergency Supplies

Talk to your co-workers about what emergency supplies the company can feasibly provide, if any, and which ones individuals should consider keeping on hand. Recommended emergency supplies include the following:

□	**Water**, amounts for portable kits will vary. Individuals should determine what amount they are able to both store comfortably and to transport to other locations. If it is feasible, store one gallon of water per person per day, for drinking and sanitation
□	**Food**, at least a three-day supply of non-perishable food
□	**Battery-powered radio** and **extra batteries**
□	**Flashlight** and **extra batteries**
□	**First Aid kit**
□	**Whistle** to signal for help
□	**Dust or filter masks**, readily available in hardware stores, which are rated based on how small a particle they filter
□	**Moist towelettes** for sanitation
□	**Wrench** or **pliers** to turn off utilities
□	**Can opener** for food (if kit contains canned food)
□	**Plastic sheeting** and **duct tape** to "seal the room"
□	**Garbage bags** and **plastic ties** for personal sanitation

Bu

- A m,

  ar

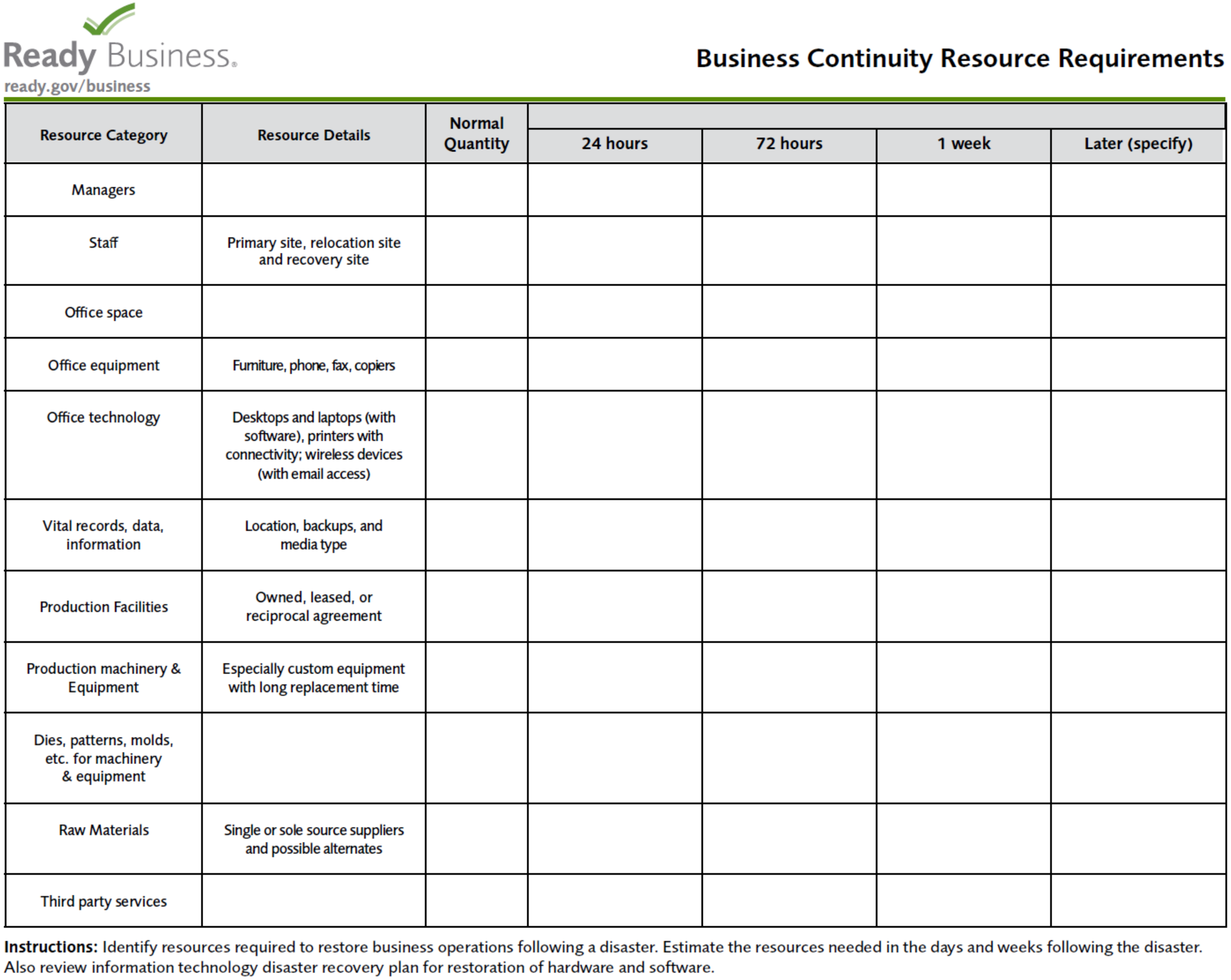
- C me

  it

  ter

  d.

- It

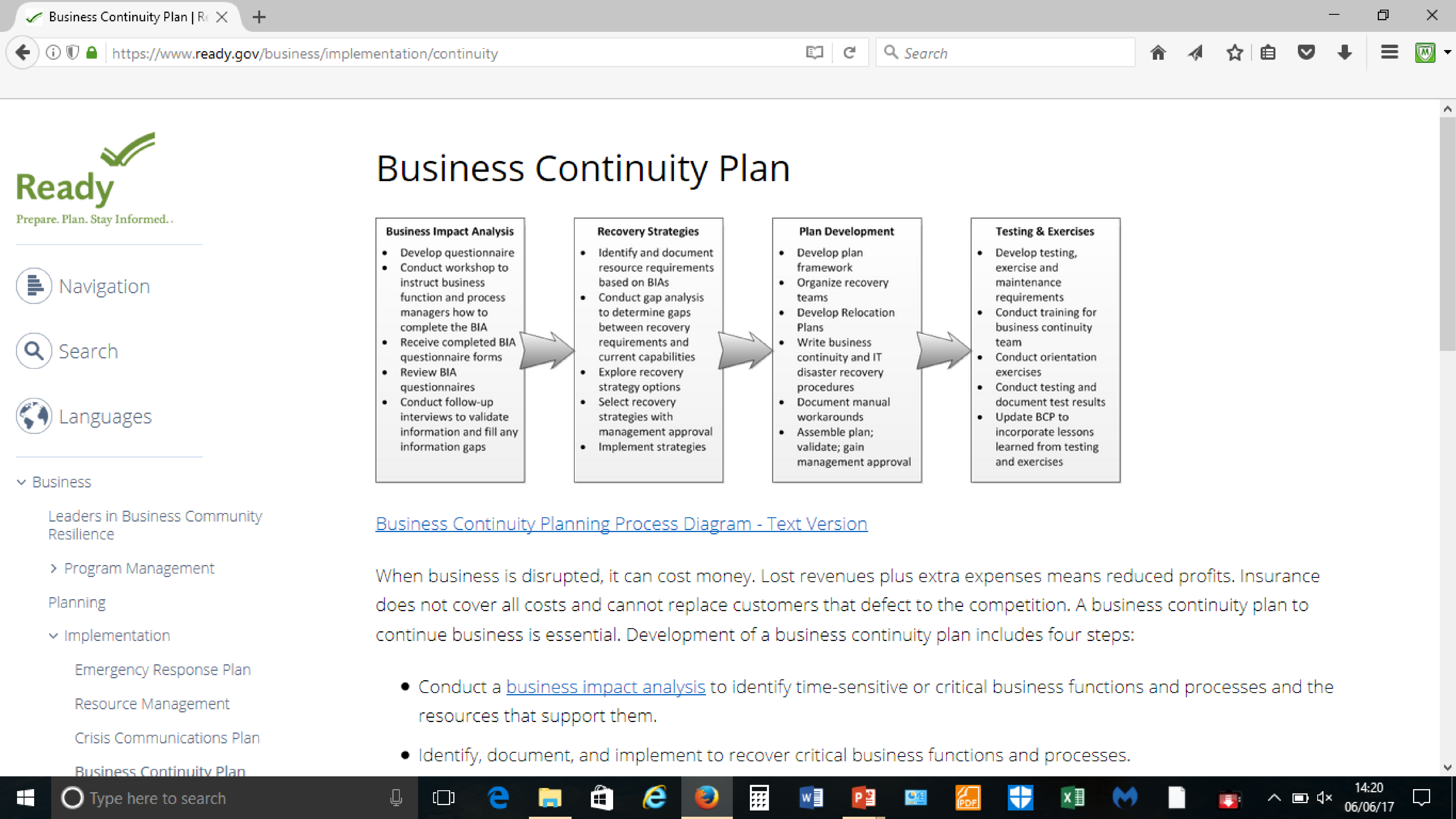


Ready Business.
ready.gov/business

Business Continuity Resource Requirements

Resource Category	Resource Details	Normal Quantity				
			24 hours	72 hours	1 week	Later (specify)
Managers						
Staff	Primary site, relocation site and recovery site					
Office space						
Office equipment	Furniture, phone, fax, copiers					
Office technology	Desktops and laptops (with software), printers with connectivity; wireless devices (with email access)					
Vital records, data, information	Location, backups, and media type					
Production Facilities	Owned, leased, or reciprocal agreement					
Production machinery & Equipment	Especially custom equipment with long replacement time					
Dies, patterns, molds, etc. for machinery & equipment						
Raw Materials	Single or sole source suppliers and possible alternates					
Third party services						

Instructions: Identify resources required to restore business operations following a disaster. Estimate the resources needed in the days and weeks following the disaster. Also review information technology disaster recovery plan for restoration of hardware and software.



Business Continuity Plan | R

https://www.ready.gov/business/implementation/continuity

Search

Ready

Prepare. Plan. Stay Informed.

Navigation

Search

Languages

Business

Leaders in Business Community Resilience

Program Management

Planning

Implementation

Emergency Response Plan

Resource Management

Crisis Communications Plan

Business Continuity Plan

Business Continuity Plan

Business Impact Analysis

- Develop questionnaire
- Conduct workshop to instruct business function and process managers how to complete the BIA
- Receive completed BIA questionnaire forms
- Review BIA questionnaires
- Conduct follow-up interviews to validate information and fill any information gaps

Recovery Strategies

- Identify and document resource requirements based on BIAs
- Conduct gap analysis to determine gaps between recovery requirements and current capabilities
- Explore recovery strategy options
- Select recovery strategies with management approval
- Implement strategies

Plan Development

- Develop plan framework
- Organize recovery teams
- Develop Relocation Plans
- Write business continuity and IT disaster recovery procedures
- Document manual workarounds
- Assemble plan; validate; gain management approval

Testing & Exercises

- Develop testing, exercise and maintenance requirements
- Conduct training for business continuity team
- Conduct orientation exercises
- Conduct testing and document test results
- Update BCP to incorporate lessons learned from testing and exercises

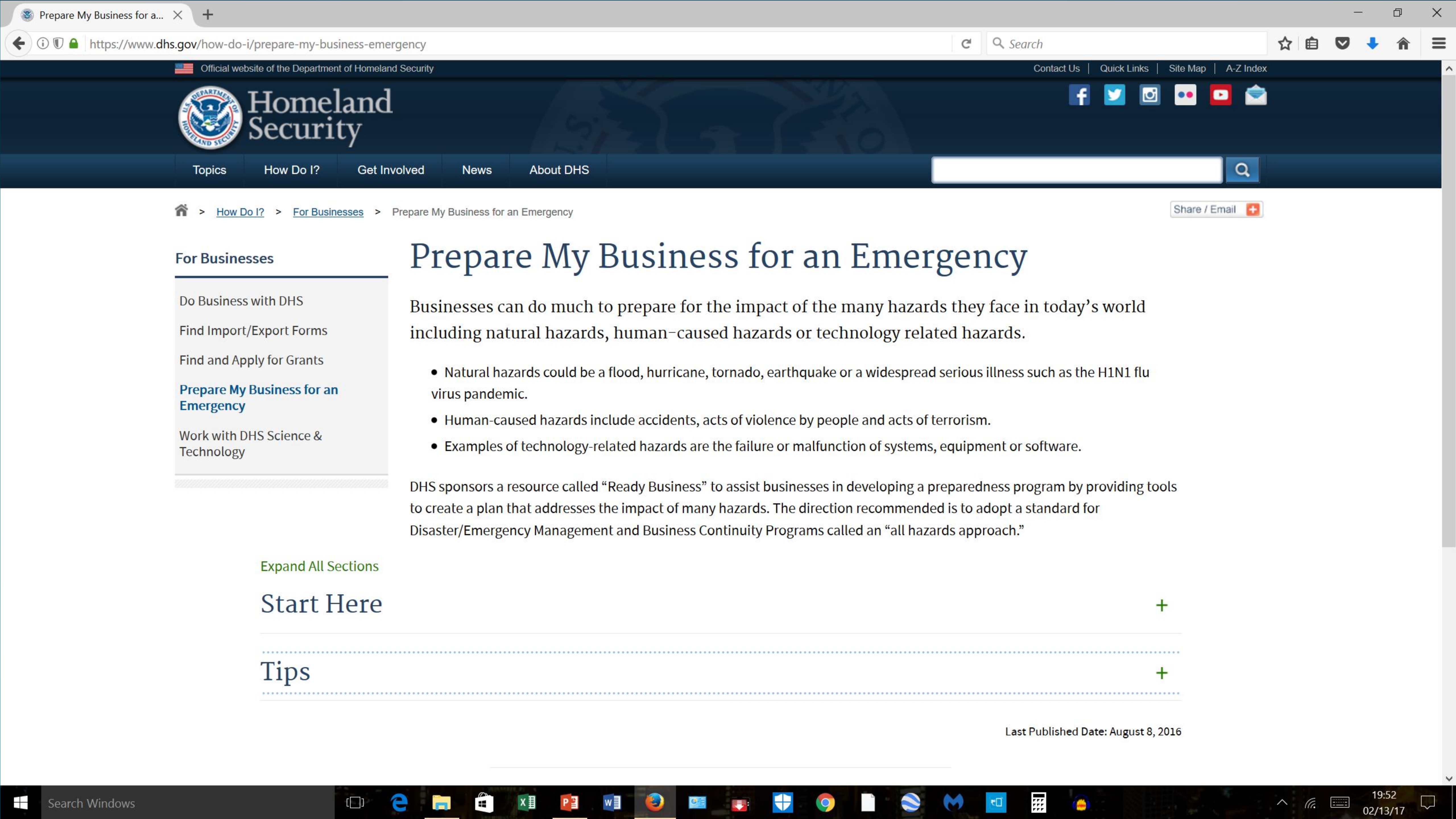
Business Continuity Planning Process Diagram - Text Version

When business is disrupted, it can cost money. Lost revenues plus extra expenses means reduced profits. Insurance does not cover all costs and cannot replace customers that defect to the competition. A business continuity plan to continue business is essential. Development of a business continuity plan includes four steps:

- Conduct a business impact analysis to identify time-sensitive or critical business functions and processes and the resources that support them.
- Identify, document, and implement to recover critical business functions and processes.

Type here to search

14:20
06/06/17


Prepare My Business for a...
https://www.dhs.gov/how-do-i/prepare-my-business-emergency
Search
Official website of the Department of Homeland Security
Contact Us | Quick Links | Site Map | A-Z Index
Homeland Security
Topics
How Do I?
Get Involved
News
About DHS
Share / Email
Search Windows
19:52
02/13/17

How Do I? > For Businesses > Prepare My Business for an Emergency

For Businesses

- Do Business with DHS
- Find Import/Export Forms
- Find and Apply for Grants
- Prepare My Business for an Emergency
- Work with DHS Science & Technology

Prepare My Business for an Emergency

Businesses can do much to prepare for the impact of the many hazards they face in today's world including natural hazards, human-caused hazards or technology related hazards.

- Natural hazards could be a flood, hurricane, tornado, earthquake or a widespread serious illness such as the H1N1 flu virus pandemic.
- Human-caused hazards include accidents, acts of violence by people and acts of terrorism.
- Examples of technology-related hazards are the failure or malfunction of systems, equipment or software.

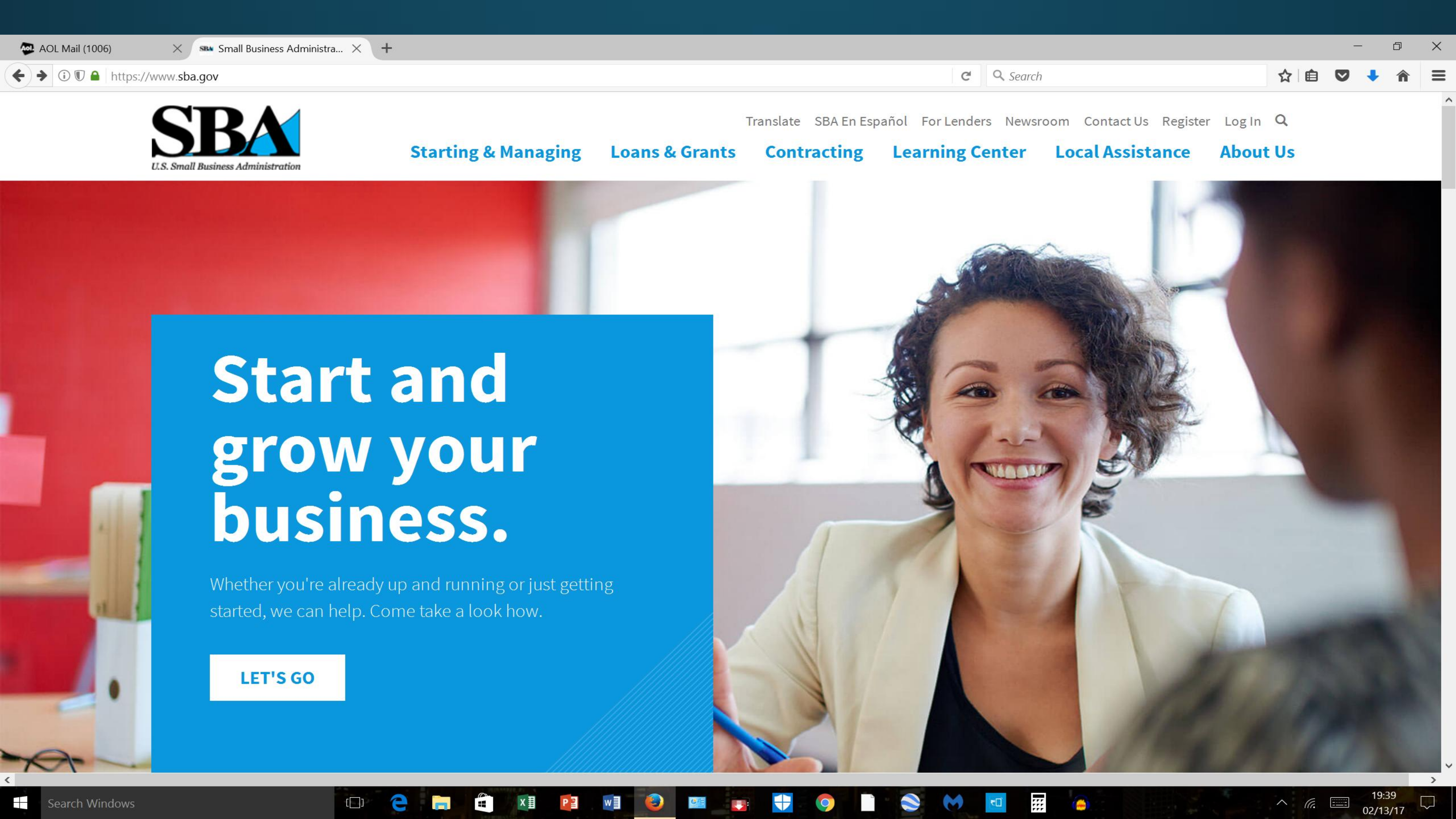
DHS sponsors a resource called "Ready Business" to assist businesses in developing a preparedness program by providing tools to create a plan that addresses the impact of many hazards. The direction recommended is to adopt a standard for Disaster/Emergency Management and Business Continuity Programs called an "all hazards approach."

Expand All Sections

Start Here +

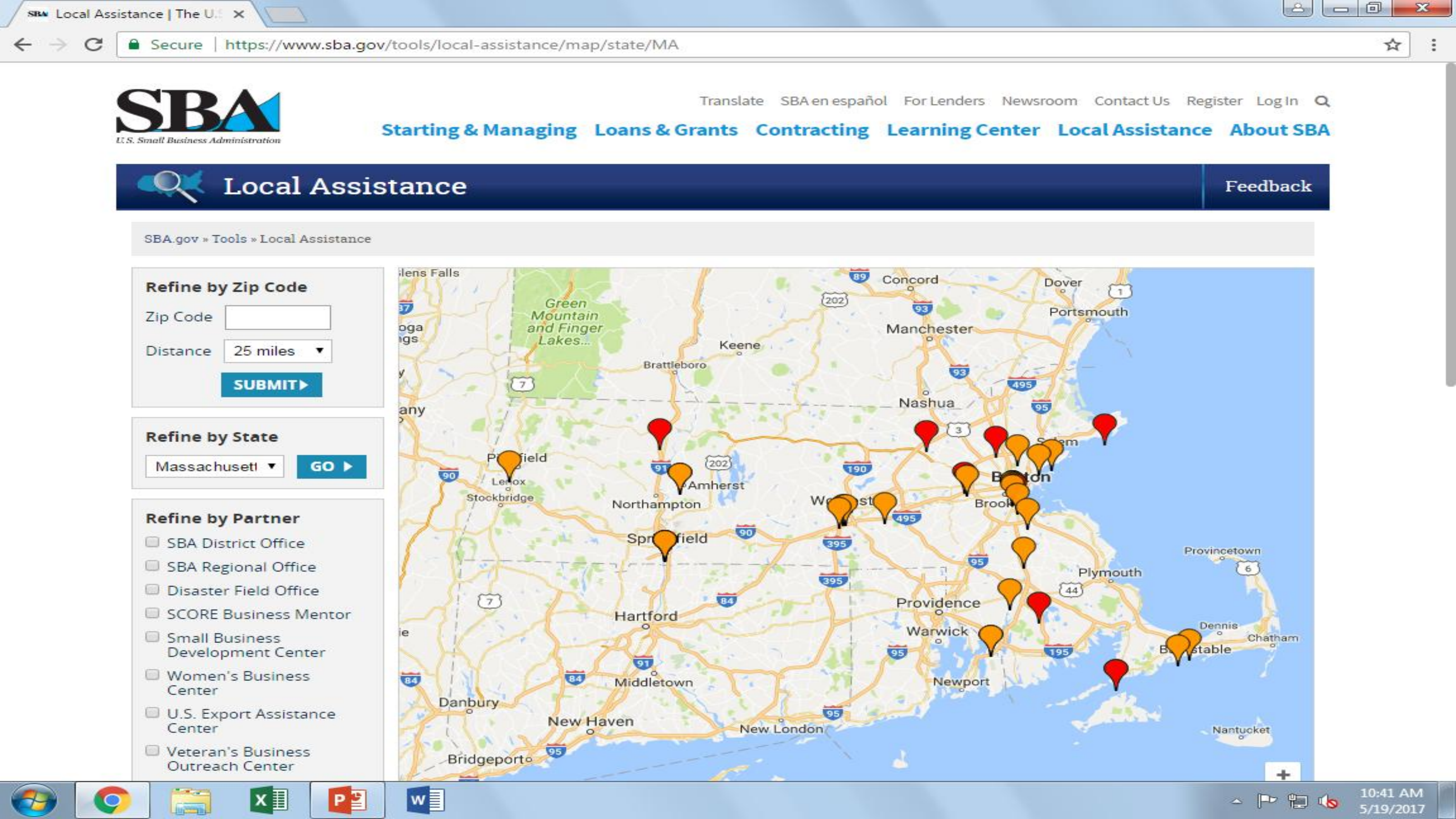
Tips +

Last Published Date: August 8, 2016



Start and grow your business.

Whether you're already up and running or just getting started, we can help. Come take a look how.



Local Assistance | The U.S

Secure | https://www.sba.gov/tools/local-assistance/map/state/MA

SBA
U.S. Small Business Administration

Translate SBA en español For Lenders Newsroom Contact Us Register Log In

Starting & Managing **Loans & Grants** **Contracting** **Learning Center** **Local Assistance** **About SBA**

Local Assistance

Feedback

SBA.gov » Tools » Local Assistance

Refine by Zip Code

Zip Code

Distance: 25 miles ▼

SUBMIT ▸

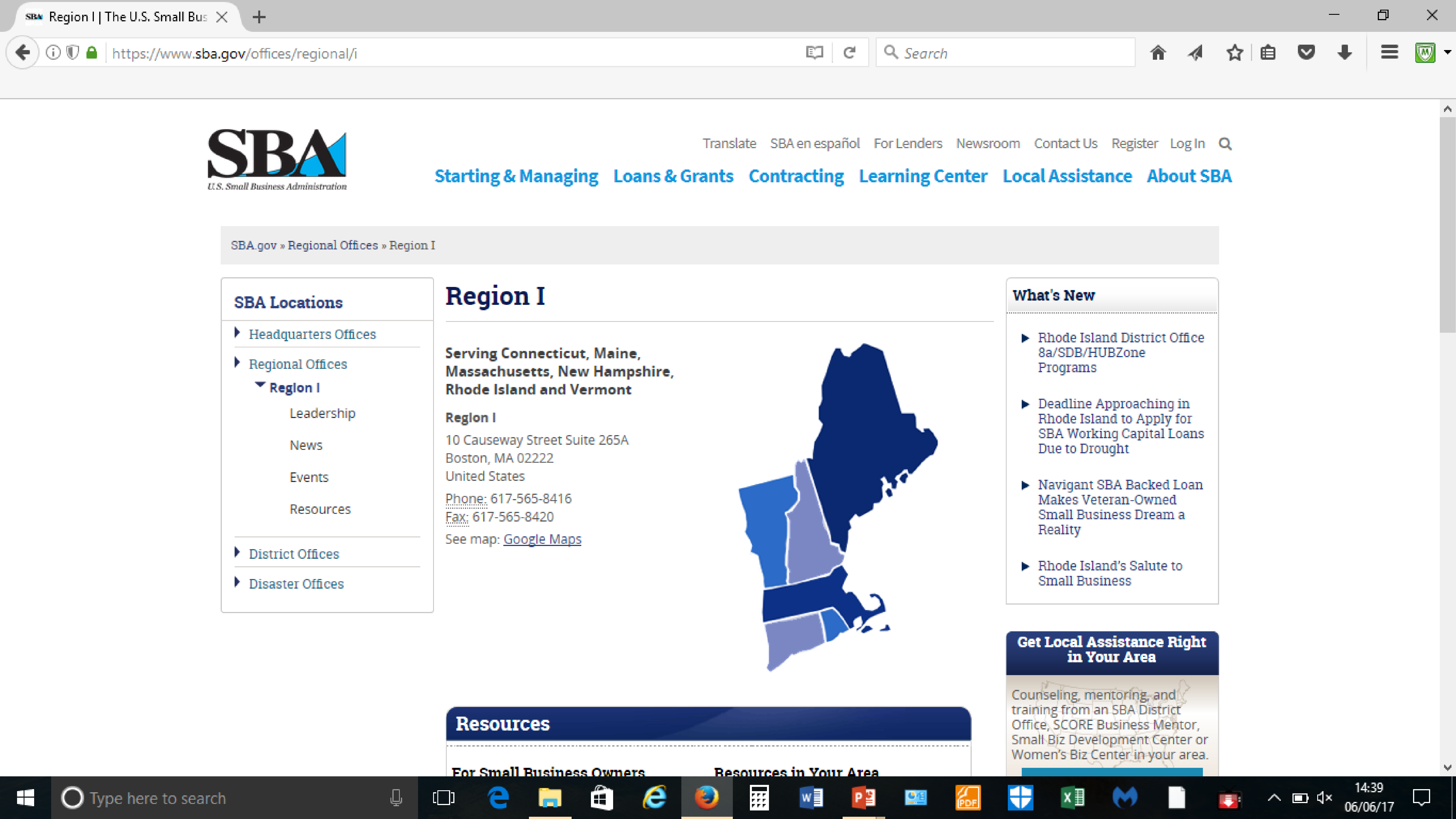
Refine by State

Massachusetts ▼ GO ▸

Refine by Partner

- □ SBA District Office
- □ SBA Regional Office
- □ Disaster Field Office
- □ SCORE Business Mentor
- □ Small Business Development Center
- □ Women's Business Center
- □ U.S. Export Assistance Center
- □ Veteran's Business Outreach Center

10:41 AM
5/19/2017



Region I | The U.S. Small Bus
https://www.sba.gov/offices/regional/i
Search

SBA
U.S. Small Business Administration

Translate SBA en español For Lenders Newsroom Contact Us Register Log In

Starting & Managing Loans & Grants Contracting Learning Center Local Assistance About SBA

SBA.gov » Regional Offices » Region I

SBA Locations

- Headquarters Offices
- Regional Offices
  - Region I
    - Leadership
    - News
    - Events
    - Resources
- District Offices
- Disaster Offices

Region I

Serving Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island and Vermont

Region I

10 Causeway Street Suite 265A
Boston, MA 02222
United States

Phone: 617-565-8416
Fax: 617-565-8420
See map: Google Maps

Resources

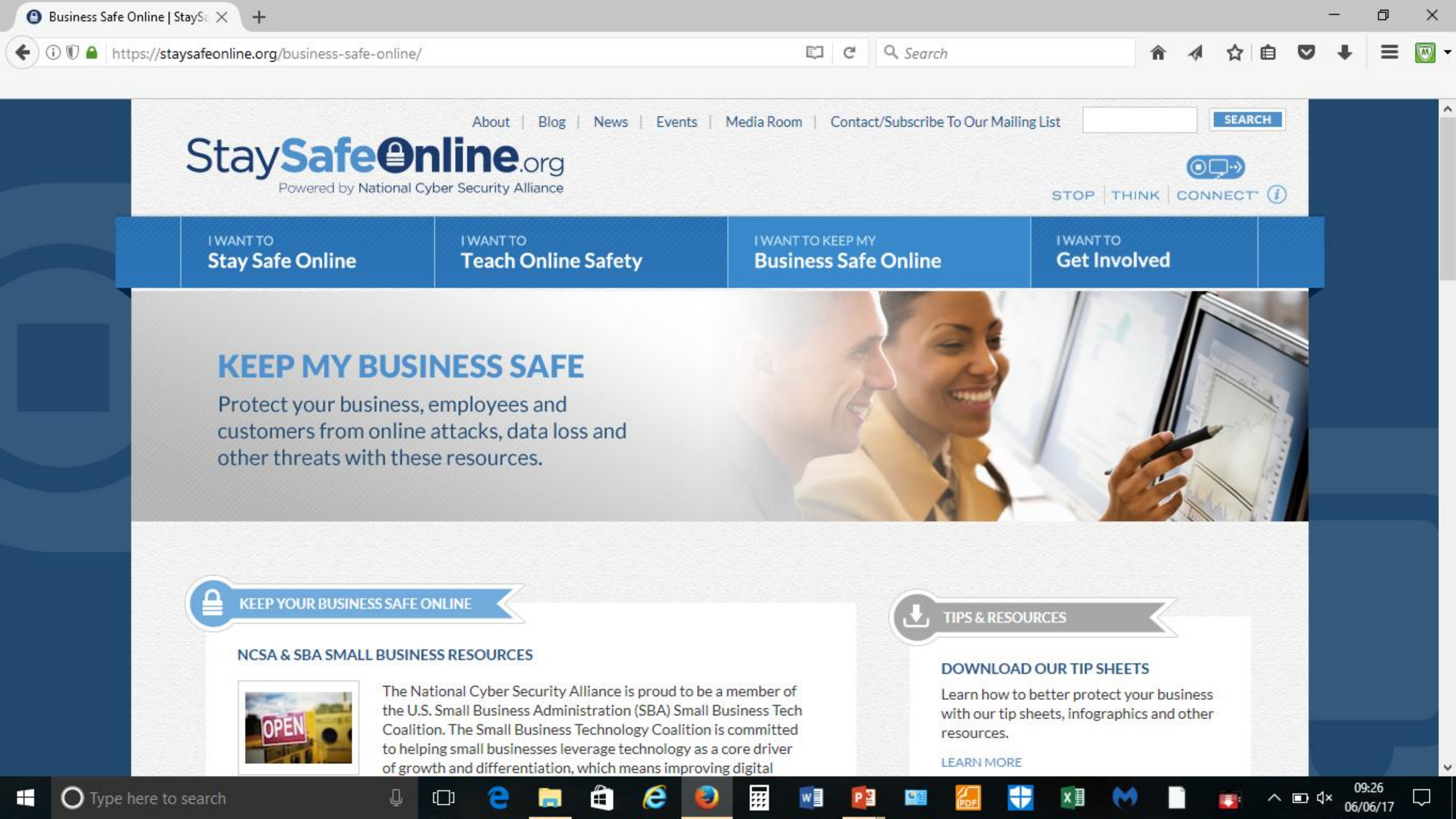
For Small Business Owners **Resources in Your Area**

What's New

- Rhode Island District Office 8a/SDB/HUBZone Programs
- Deadline Approaching in Rhode Island to Apply for SBA Working Capital Loans Due to Drought
- Navigant SBA Backed Loan Makes Veteran-Owned Small Business Dream a Reality
- Rhode Island's Salute to Small Business

Get Local Assistance Right in Your Area

Counseling, mentoring, and training from an SBA District Office, SCORE Business Mentor, Small Biz Development Center or Women's Biz Center in your area.


Business Safe Online | StaySa
https://staysafeonline.org/business-safe-online/
Search
About | Blog | News | Events | Media Room | Contact/Subscribe To Our Mailing List
SEARCH
StaySafeOnline.org
Powered by National Cyber Security Alliance
STOP | THINK | CONNECT
I WANT TO Stay Safe Online
I WANT TO Teach Online Safety
I WANT TO KEEP MY Business Safe Online
I WANT TO Get Involved
OPEN
Type here to search
09:26
06/06/17

KEEP MY BUSINESS SAFE

Protect your business, employees and customers from online attacks, data loss and other threats with these resources.

KEEP YOUR BUSINESS SAFE ONLINE

NCSA & SBA SMALL BUSINESS RESOURCES

The National Cyber Security Alliance is proud to be a member of the U.S. Small Business Administration (SBA) Small Business Tech Coalition. The Small Business Technology Coalition is committed to helping small businesses leverage technology as a core driver of growth and differentiation, which means improving digital

TIPS & RESOURCES

DOWNLOAD OUR TIP SHEETS

Learn how to better protect your business with our tip sheets, infographics and other resources.

LEARN MORE

SBA Offers Ten Cybersecurity Tips

- Protect against viruses, spyware, and other malicious code
- Secure your networks
- Establish security practices and policies to protect sensitive information
- Educate employees about cyberthreats and hold them accountable

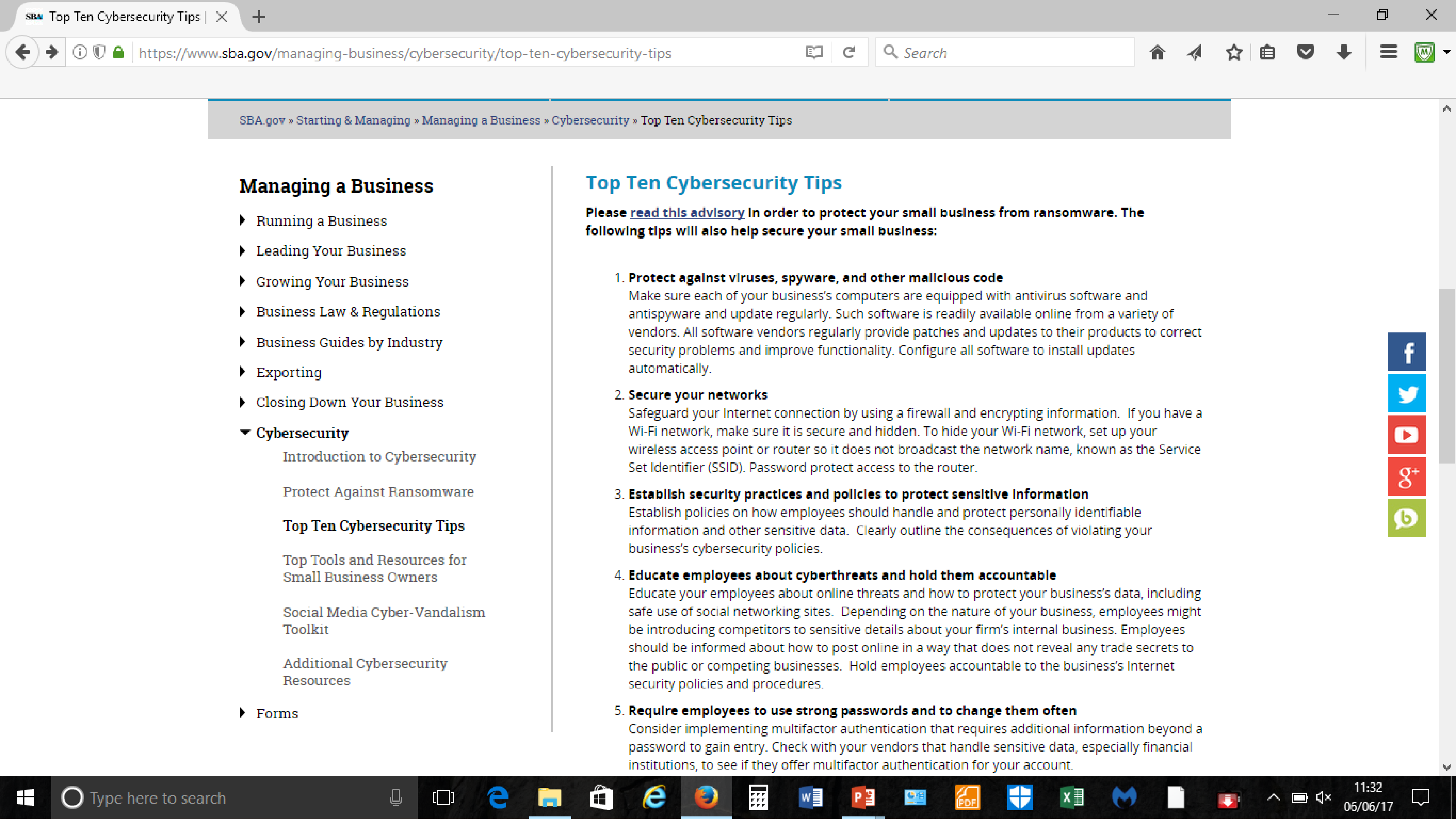
https://www.sba.gov/managing-business/cybersecurity/top-ten-cybersecurity-tips

SBA Offers Ten Cybersecurity Tips

- Require employees to use strong passwords and to change them often
- Employ best practices on payment cards
- Make backup copies of important business data and information

SBA Offers Ten Cybersecurity Tips

- Control physical access to computers and network components
- Create a mobile device action plan
- Protect all pages on your public-facing websites, not just the checkout and sign-up pages


Top Ten Cybersecurity Tips |
https://www.sba.gov/managing-business/cybersecurity/top-ten-cybersecurity-tips
Search
Type here to search
11:32
06/06/17

SBA.gov » Starting & Managing » Managing a Business » Cybersecurity » Top Ten Cybersecurity Tips

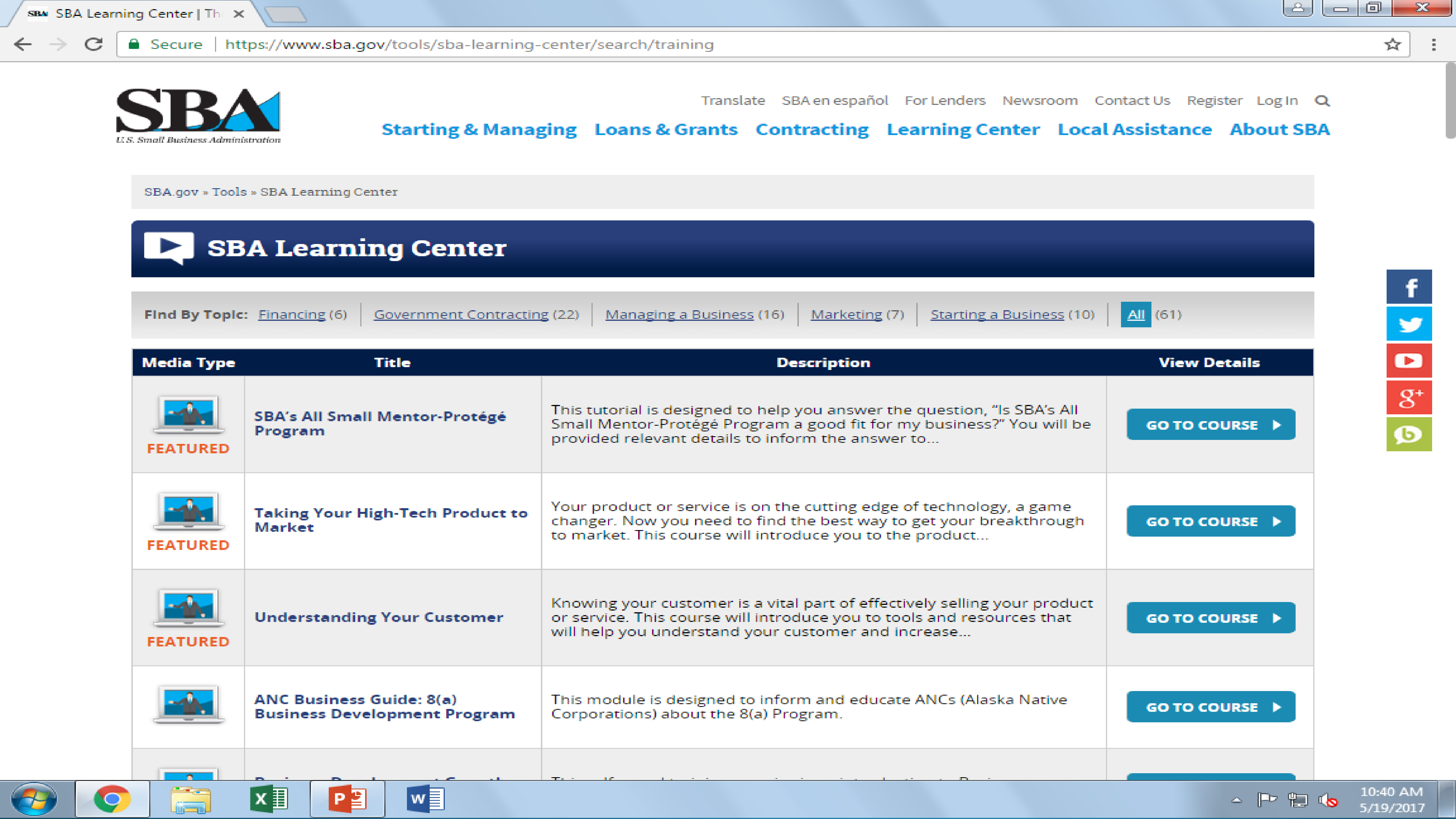
Managing a Business

- Running a Business
- Leading Your Business
- Growing Your Business
- Business Law & Regulations
- Business Guides by Industry
- Exporting
- Closing Down Your Business
- Cybersecurity
  - Introduction to Cybersecurity
  - Protect Against Ransomware
  - **Top Ten Cybersecurity Tips**
  - Top Tools and Resources for Small Business Owners
  - Social Media Cyber-Vandalism Toolkit
  - Additional Cybersecurity Resources
- Forms

Top Ten Cybersecurity Tips

Please read this advisory in order to protect your small business from ransomware. The following tips will also help secure your small business:

1. **Protect against viruses, spyware, and other malicious code**
   Make sure each of your business's computers are equipped with antivirus software and antispyware and update regularly. Such software is readily available online from a variety of vendors. All software vendors regularly provide patches and updates to their products to correct security problems and improve functionality. Configure all software to install updates automatically.
2. **Secure your networks**
   Safeguard your Internet connection by using a firewall and encrypting information. If you have a Wi-Fi network, make sure it is secure and hidden. To hide your Wi-Fi network, set up your wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID). Password protect access to the router.
3. **Establish security practices and policies to protect sensitive information**
   Establish policies on how employees should handle and protect personally identifiable information and other sensitive data. Clearly outline the consequences of violating your business's cybersecurity policies.
4. **Educate employees about cyberthreats and hold them accountable**
   Educate your employees about online threats and how to protect your business's data, including safe use of social networking sites. Depending on the nature of your business, employees might be introducing competitors to sensitive details about your firm's internal business. Employees should be informed about how to post online in a way that does not reveal any trade secrets to the public or competing businesses. Hold employees accountable to the business's Internet security policies and procedures.
5. **Require employees to use strong passwords and to change them often**
   Consider implementing multifactor authentication that requires additional information beyond a password to gain entry. Check with your vendors that handle sensitive data, especially financial institutions, to see if they offer multifactor authentication for your account.

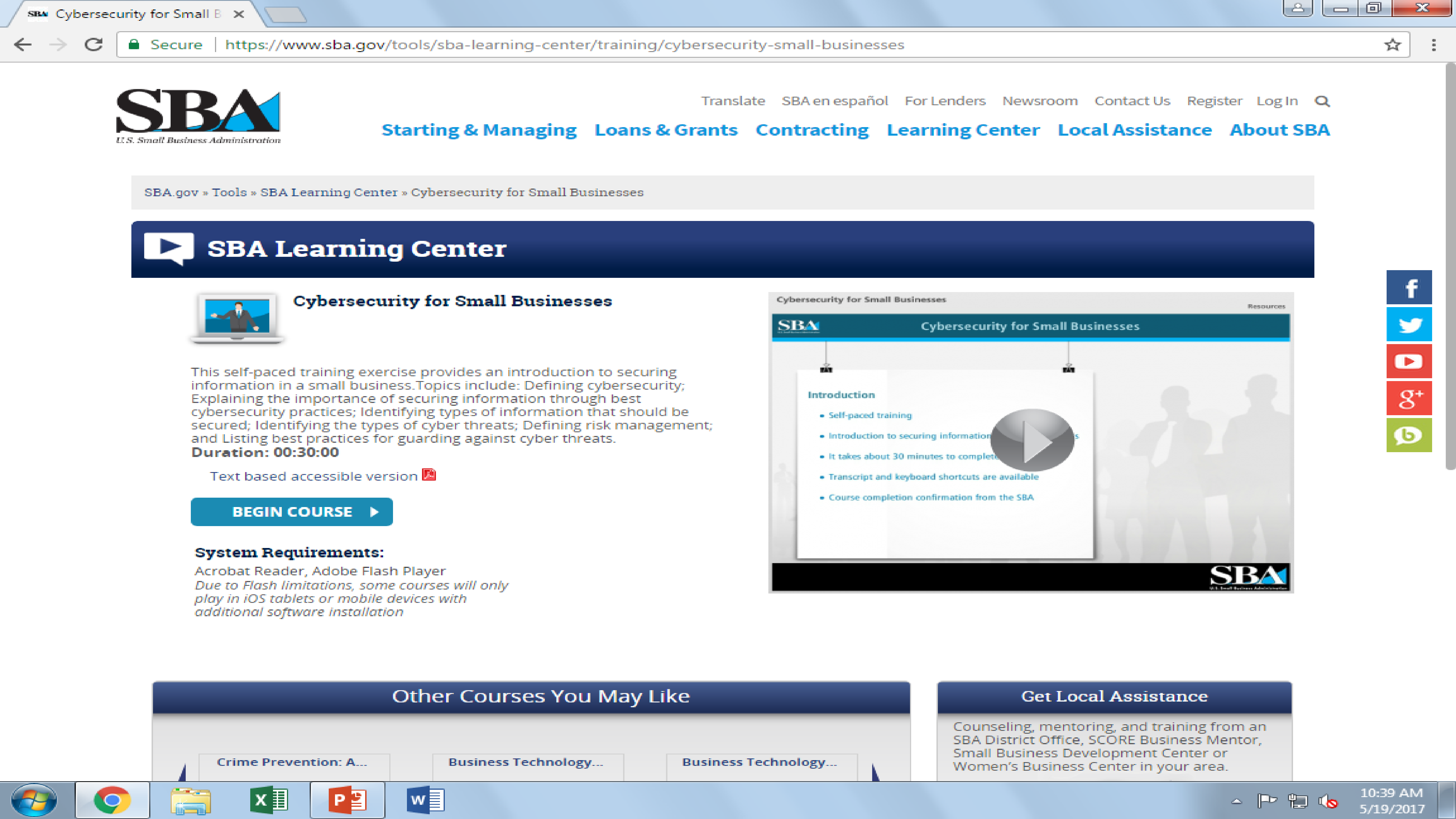


SBA.gov » Tools » SBA Learning Center

SBA Learning Center

Find By Topic: Financing (6) | Government Contracting (22) | Managing a Business (16) | Marketing (7) | Starting a Business (10) | All (61)

Media Type	Title	Description	View Details
FEATURED	**SBA's All Small Mentor-Protégé Program**	This tutorial is designed to help you answer the question, "Is SBA's All Small Mentor-Protégé Program a good fit for my business?" You will be provided relevant details to inform the answer to...	GO TO COURSE ▶
FEATURED	**Taking Your High-Tech Product to Market**	Your product or service is on the cutting edge of technology, a game changer. Now you need to find the best way to get your breakthrough to market. This course will introduce you to the product...	GO TO COURSE ▶
FEATURED	**Understanding Your Customer**	Knowing your customer is a vital part of effectively selling your product or service. This course will introduce you to tools and resources that will help you understand your customer and increase...	GO TO COURSE ▶
	ANC Business Guide: 8(a) Business Development Program	This module is designed to inform and educate ANCs (Alaska Native Corporations) about the 8(a) Program.	GO TO COURSE ▶



SBA.gov » Tools » SBA Learning Center » Cybersecurity for Small Businesses

SBA Learning Center

Cybersecurity for Small Businesses

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

Duration: 00:30:00

Text based accessible version

BEGIN COURSE ▶

System Requirements:

Acrobat Reader, Adobe Flash Player

Due to Flash limitations, some courses will only play in iOS tablets or mobile devices with additional software installation

Cybersecurity for Small Businesses
Resources
Cybersecurity for Small Businesses
Introduction
Self-paced training
Introduction to securing information
It takes about 30 minutes to complete
Transcript and keyboard shortcuts are available
Course completion confirmation from the SBA

Other Courses You May Like

Crime Prevention: A...

Business Technology...

Business Technology...

Get Local Assistance

Counseling, mentoring, and training from an SBA District Office, SCORE Business Mentor, Small Business Development Center or Women's Business Center in your area.

DHS Chemical Facility Preparedness Program (CFATS)

- The Chemical Facility Anti-Terrorism Standards (CFATS) program identifies and regulates high-risk chemical facilities to ensure they have security measures in place to reduce the risks associated with these chemicals.
- 16 page Appendix of chemicals of interest.
- Concern of sabotage, theft, release.

DHS Chemical Facility Anti-Terrorism Standards (CFATS)
http://www.dhs.gov/chemical-facility-anti-terrorism-standards

Local Assets for Preparation/Response

- Fire
- Police
- EMS
- Public Health
- Public Works
- Emergency Management

Photo credit: http://www.rand.org/

Summary

All types of businesses need to be prepared for interruptions.

Natural causes, deliberate acts, attacks from within and industrial espionage are areas of vulnerability.

Performing a risk assessment and mitigation plan may contribute to continuity of operations and/or rapid recovery and return to production.

Summary

- A variety of resources are available:
- FEMA
- DHS
- SBA all offer guidance on preparation and response.

Questions?

Evaluation Information

Bob Zalewski

bzalewski@nhcosh.org