Wisconsin Procurement Institute

A Procurement Technical Assistance Center (PTAC)

TOOLS, PRACTICES AND RESOURCES FOR YOUR CYBER-SECURITY TOOLBOX

Cyber Friday Webinar

November 6, 2020




ABOUT WPI
SUPPORTING THE MISSION

Celebrating 32 Years of serving Wisconsin Business!

WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

Assist businesses in creating, developing and growing their sales, revenue and jobs through Federal, State and Local Government contracts.

- **INDIVIDUAL COUNSELING – At our offices, at client's facility or via telephone/GoToWebinar**
- **SMALL GROUP TRAINING – Workshops and webinars**
- **CONFERENCES to include one on one or roundtable sessions**

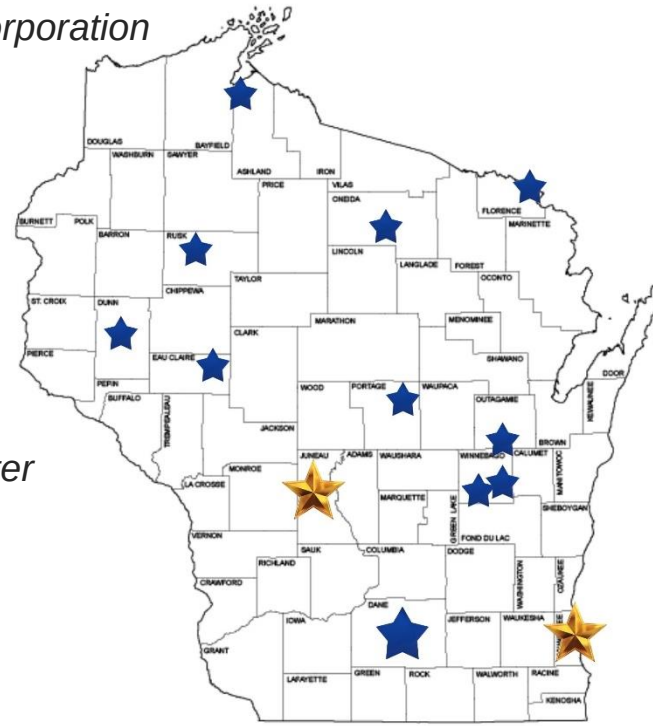
Last year WPI provided training at over 100 events and provided service to over 1,200 companies

WPI is a Procurement Technical Assistance Center (PTAC) funded in part by the Defense Logistics Agency (DLA), WEDC and other funding sources.

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

WPI OFFICE LOCATIONS

- **MILWAUKEE**
  - *Technology Innovation Center*
- **MADISON**
  - *FEED Kitchens*
  - *Dane County Latino Chamber of Commerce*
  - *Wisconsin Manufacturing Extension Partnership (WMEP)*
  - *Madison Area Technical College (MATC)*
- **CAMP DOUGLAS**
  - *Juneau County Economic Development Corporation (JCEDC)*
- **STEVENS POINT**
  - *IDEA Center*
- **APPLETON**
  - *Fox Valley Technical College*
- **FLORENCE**
  - *Florence County Economic Development*
- **OSHKOSH**
  - *Fox Valley Technical College*
  - *Greater Oshkosh Economic Development Corporation*
- **EAU CLAIRE**
  - *Western Dairyland*
- **MENOMONIE**
  - *Dunn County Economic Development Corporation*
- **LADYSMITH**
  - *Indianhead Community Action Agency*
- **RHINELANDER**
  - *Nicolet Area Technical College*
- **GREEN BAY**
  - *Advance Business & Manufacturing Center*
- **ASHLAND**
  - *Ashland Area Development Corporation*



Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

11/6/20


Search ...
BLOG
SERVICES
ABOUT
CLIENT PORTAL
SPONSORSHIP
CONTACT
Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
EVENT CALENDAR
FEDERAL GOVERNMENT
STATE & LOCAL GOVERNMENT
GRANTS
SUCCESS & AWARDS
FAQS
CURRENT EDITION OF THE WPI NEWSLETTER
UPCOMING EVENTS
WED 21
Acquisition Hour: Government Property Management for Federal Contractors and Subcontractors
August 21 @ 12:00 pm - 1:00 pm
THU 22
Advancing Cybersecurity in the Industry, Energy, Water Nexus – Oshkosh, WI
August 22 @ 9:00 am - 3:00 pm
Oshkosh WI
THU 22
NDIA Great Lakes Chapter 10th Anniversary – Milwaukee, WI
August 22 @ 12:30 pm - 7:30 pm
Brookfield Wisconsin
SEP 11
Acquisition Hour: The End of the Fiscal Year is Here – What is Hot and What is Not
September 11 @ 12:00 pm - 1:00 pm
View More...
CURRENT OPPORTUNITIES (1)
www.wispro.org
GET STARTED WITH THE BASICS
Questions & answers on how to get started.
SIGN-UP FOR OUR NEWSLETTER
Stay up-to-date with the latest WPI news.
HAVE A QUESTION? WE'RE HERE TO HELP.
One of our staff of experts is available to answer your questions.

TOOLS, PRACTICES AND RESOURCES FOR YOUR CYBER-SECURITY TOOLBOX

Marc N. Violante

Wisconsin Procurement Institute

November 6, 2020

WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

OVERVIEW

- Cybersecurity is not a "thing" or just a plan or some other end-result that once completed never sees the light of day.
- Cybersecurity requires vigilance, awareness and an array of knowledge, tools and skills tailored for every level of the organization and which are practiced on a daily basis.

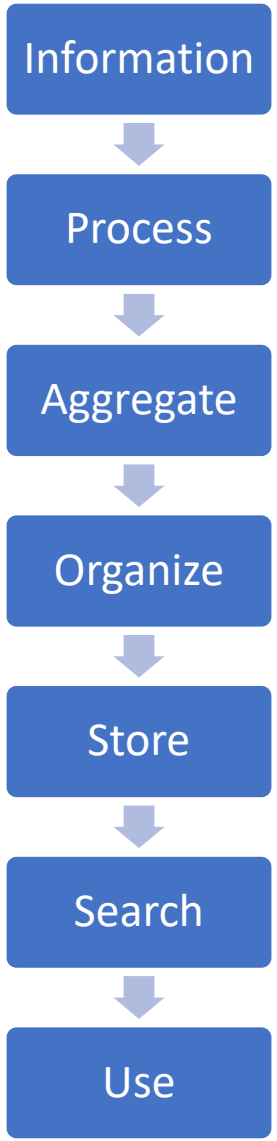
There is a treasure trove of relevant, accessible and useful information on the web. The key issues are:

- Locating it
- Determining it’s value
- Determining whether it is credible
- Saving it
- Sorting it
- Creating a functional and usable knowledge system

Key issues

There is a treasure trove of relevant, accessible and useful information on the web.

The key issues are:



Objectives

- Tools for the toolbox | kitchen drawer | garage | etc
  - Collection of related and useful items
  - General theme, not specific to one narrow topic | subject
- Goals
  - Free – publicly accessible – maybe registration is required
  - Credible
  - Useful – provides usable information/resources
  - Outline a framework or pathway in moving forward
  - Resources to help stay current

- Why is current important?

The need to stay current!

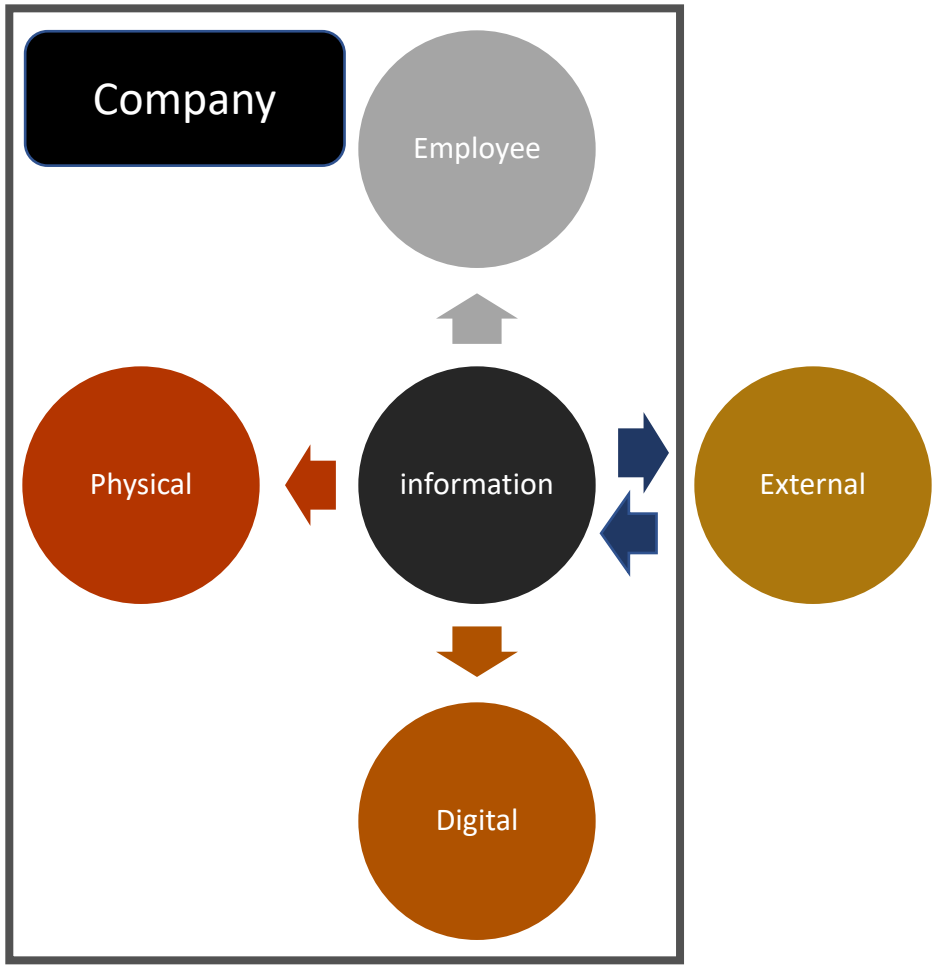
Hackers used previously unknown tools in a cyber espionage campaign targeting defence and aerospace companies in a social engineering and phishing campaign which is more widely targeted than first thought.

Researchers at McAfee first detailed Operation North Star earlier this year, but further analysis of reveals additional tactics and techniques of the campaign which has almost identical elements to Hidden Cobra – AKA The Lazarus Group – a hacking operation which the US government and others say is working out of North Korea on behalf of the government in Pyongyang.

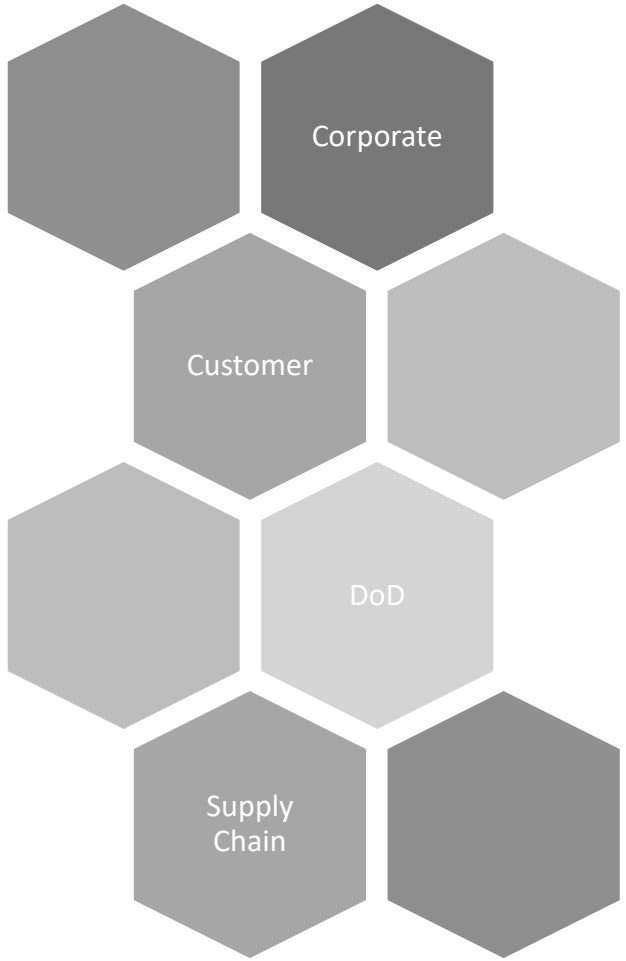
The campaign is still based around spear-phishing emails and LinkedIn messages which pose as job recruitment messages in an effort to lure victims into opening malicious attachments. Hackers

https://www.zdnet.com/article/this-hacking-group-is-using-previously-unknown-tools-to-target-defence-contractors/?ftag=TRE-03-10aaa6b&bhid=291855109939622478424925253825 82&mid=13155635&cid=2227112790

Information flows



General Information Sources



Security Perimeter/Programs

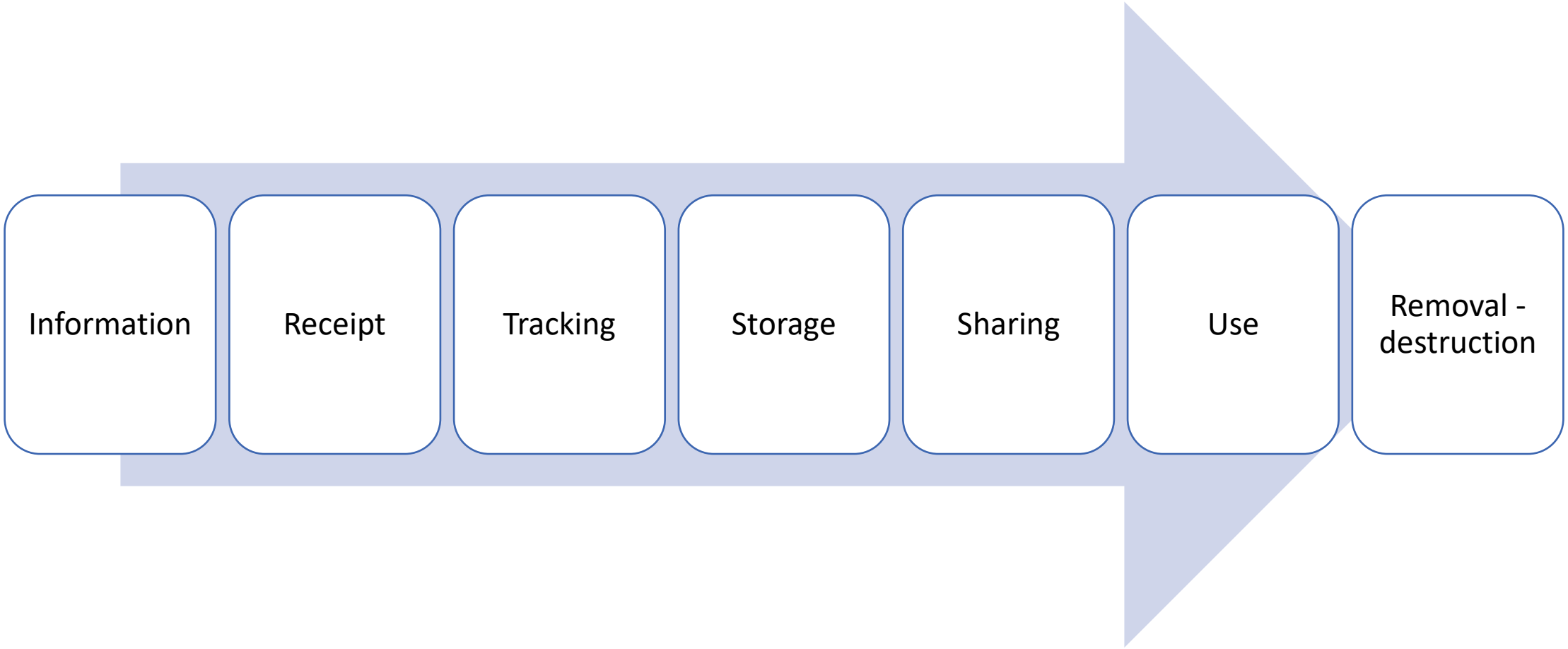
Information – general categories of use

Brought in	Created	Copied	Shared
Destroyed	Lost	Used	Retained

General Handling Considerations

- What qualifies
- Information life-cycle
- Registrations
- Company policies
- Company POC’s
- Marking
- Storage
- Sharing
- Communication channels
- Retention
- Destruction
- Incident requirements
- Special considerations
- Training requirements

Information usage lifecycle



Business Functions impacted

- Sales
- Marketing
- Web Design/External Communications
- Engineering
- Operations
- Purchasing
- Business Development
- Human Resources
- Finance – Invoice, AR
- Service contracting (external)
- Information Technology

Key Tools

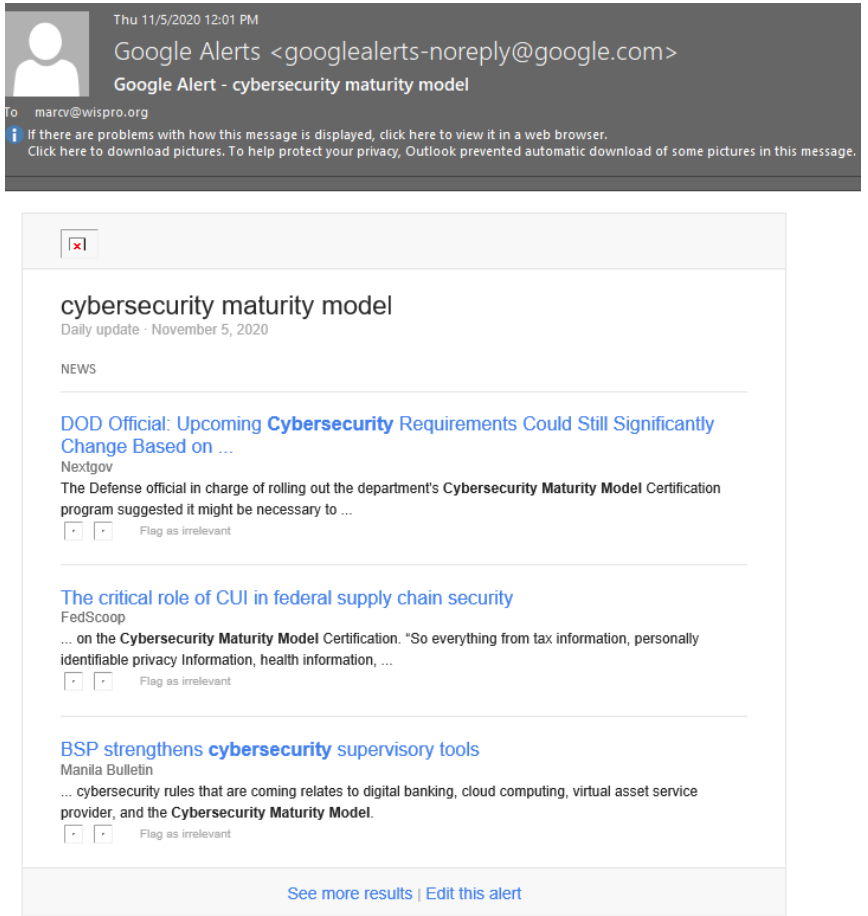
- Caution
- Awareness
- Deliberateness
- Thoughtfulness
- Training
- Engagement
- Resources

- Policies
- Procedures
- Communications

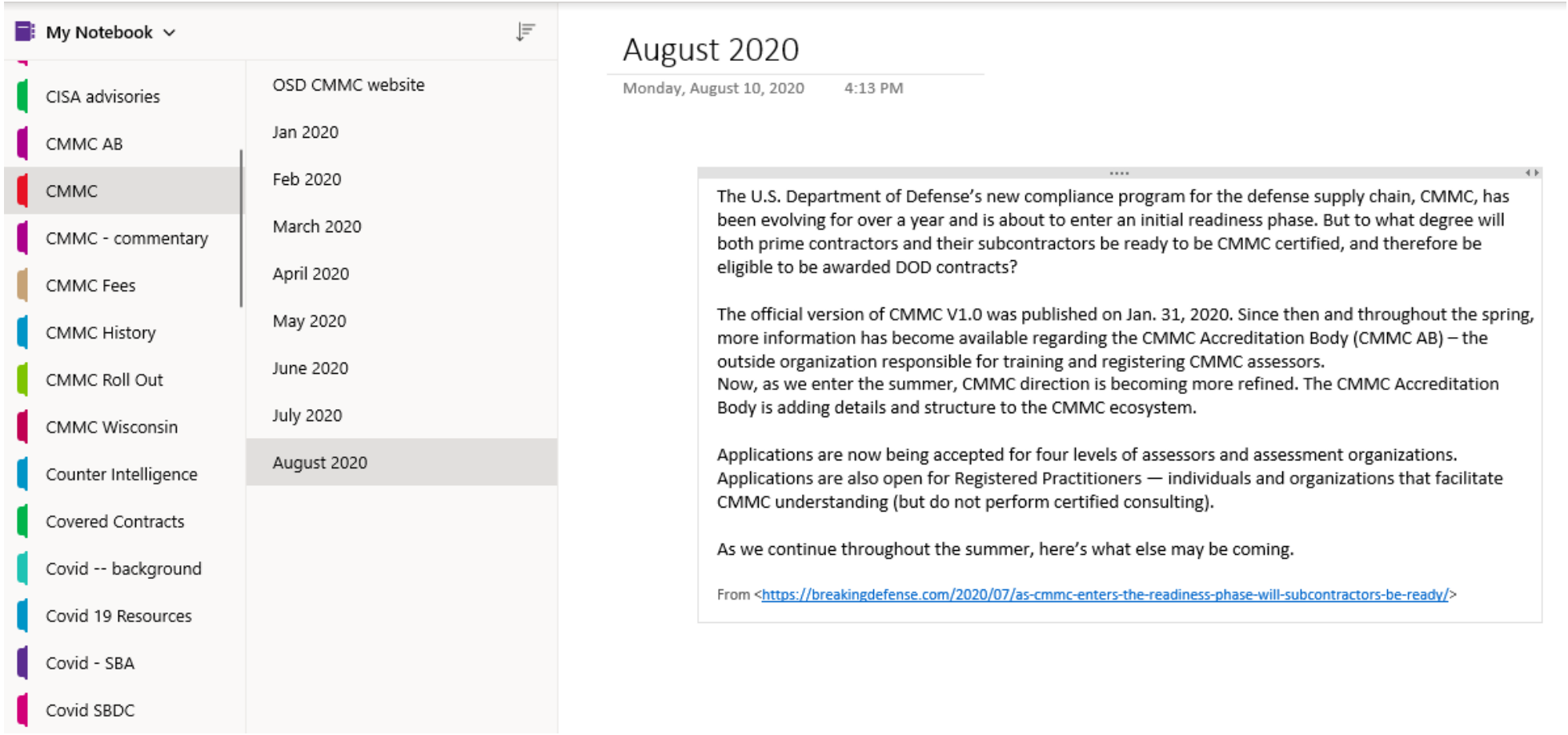
Develop Project Timeline

- Define starting point
- Define parameters – boundaries – framework
- Create “work break-down structure”
- Assign responsibility
- Prioritize
- Develop communication mechanism
- Identify critical path
  - Identify critical needs – funding, talent, resources, time

Google Alerts



Tools to store, organize and access



“There’s a truism in cybersecurity that you can’t protect what you can’t detect,” Richberg said. “And I’d say there’s a corollary to that, and it’s hard to protect what you don’t understand.

So if you don’t genuinely understand the sensitivity the government ascribes to a given piece or category information, it’s really hard to know how to treat it.”

https://www.fedscoop.com/critical-role-cmmc-federal-supply-chain-security/

“Run to ground” as a general philosophy

- Ideas
- Terms
- Requirements
- Fully understand; document; references; exhaust resources
- If you don’t absolutely know or understand what is specifically required, then what can be said about the solution?

Identify system topology (footprint)

- Network
- Subset
- enclave

Network Segmentation versus Network Enclaving

Tweet As we have discussed in earlier blogs, network segmentation is the practice of splitting computer networks into subnets using combinations of firewalls, VLANs, access controls and policies & procedures. We have seen that the primary reason for segmenting networks is to prevent a simple perimeter breach from exposing the totality of an organization's information assets. So what is the difference between network segmentation and network enclaving?

One of the differences is just the degree of segmentation you impose upon the network. Enclaves are more thoroughly segmented from the general network environment than usual. In fact, enclaving is sometimes just described as "enhanced network segmentation."

Another difference between segmentation and enclaving is the primary threat enclaving strives to thwart: the internal threat. Although the preponderance of cyber-attacks come from external threat sources such as hackers, cyber-criminals and nation states, many of the most devastating breaches originate from internal sources such as employees and trusted service providers. These internal information security breaches may be either purposeful attacks or may simply be caused by employee error. Either way, they are just as devastating to an organization's reputation and business share.

https://stateofsecurity.com/network-segmentation-versus-network-enclaving/

Create/Develop baselines

- Personnel
  - Knowledge
  - Skills
  - Functional expertise
  - Gaps
- Requirements
- Equipment
  - functionality

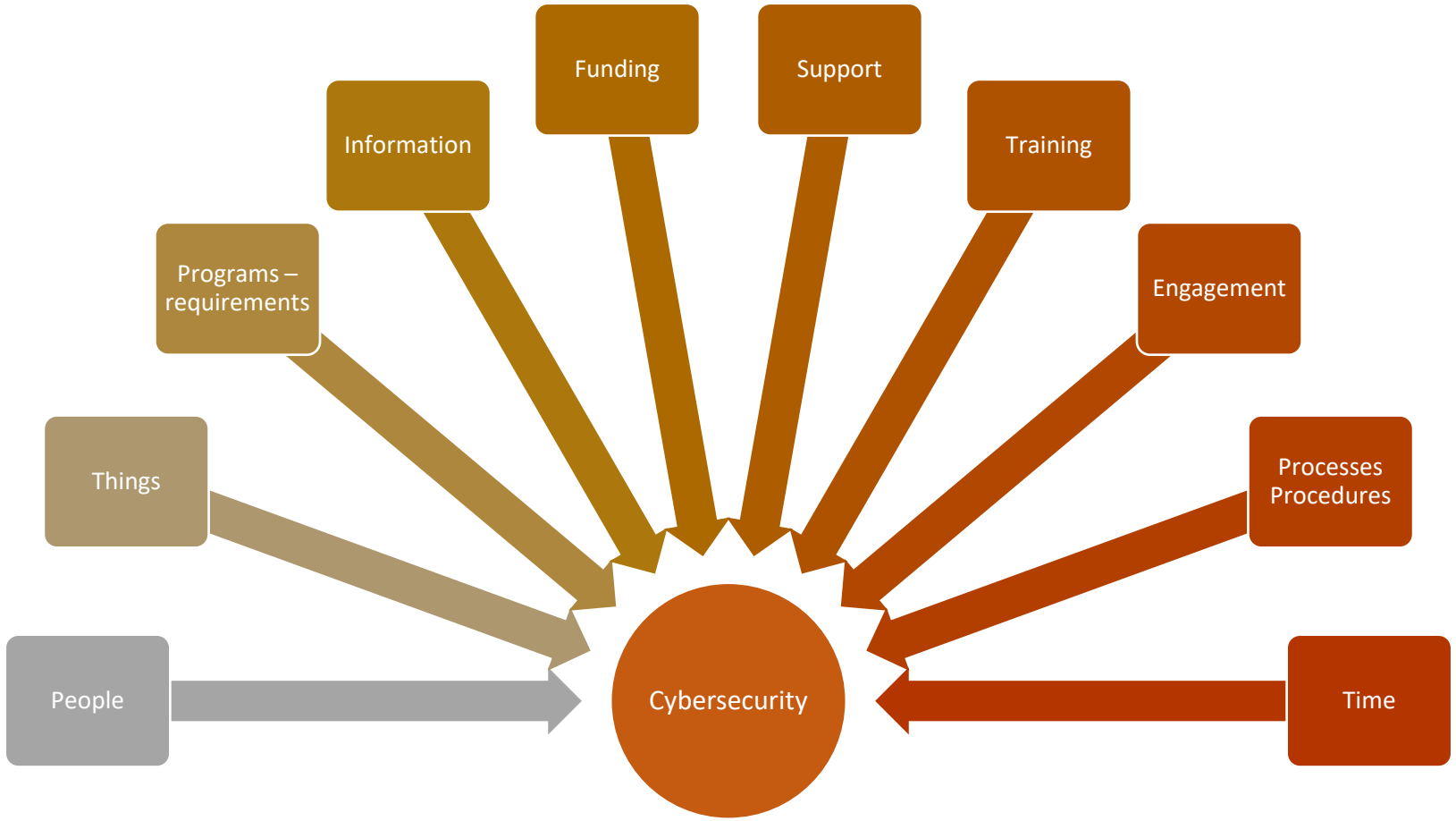
Programs/Requirements

- Federal Contract Information
- Controlled Unclassified Information
- Export Controlled
- JCP
- NOFORN
- Customer – commercial restricted/proprietary
- Corporate - proprietary

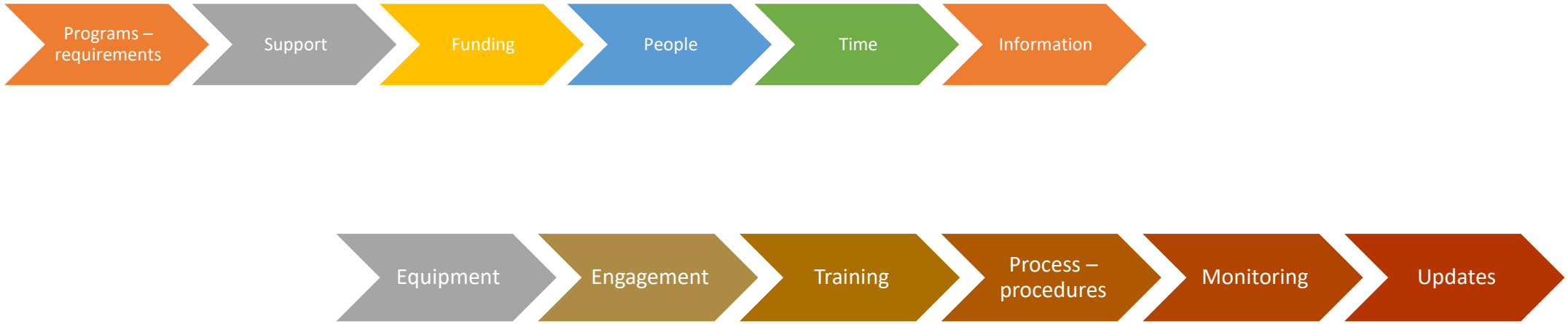
Identify requirements – information in-house

- Contractual requirements/obligations
- Information used, stored, shared
- Determine retention requirements
  - Destroy (as appropriate)
  - Reduce – information footprint

Categorize Resource types



Identify the Driver(s) (example)



Understand “belief system”

- Dangers of smoking
- Dangers of texting and driving
- Dangers of mountain biking
- Dangers of coronavirus
- Dangers of being hacked
- Dangers of cyber attacks

Official website of the Department of Homeland Security

US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

5 Questions CEOs Should Ask About Cyber Risks

1) How Is Our Executive Leadership Informed About the Current Level and Business Impact of Cyber Risks to Our Company?
2) What Is the Current Level and Business Impact of Cyber Risks to Our Company? What Is Our Plan to Address Identified Risks?
3) How Does Our Cybersecurity Program Apply Industry Standards and Best Practices?
4) How Many and What Types of Cyber Incidents Do We Detect In a Normal Week? What is the Threshold for Notifying Our Executive Leadership?
5) How Comprehensive Is Our Cyber Incident Response Plan? How Often Is It Tested?

What should CEOs know about the cybersecurity threats their companies face?

CEOs should ask the following questions about potential cybersecurity threats:

- How could cybersecurity threats affect the different functions of my business, including areas such as supply chain, public relations, finance, and human resources?
- What type of critical information could be lost (e.g., trade secrets, customer data, research, personally identifiable information)?
- How can my business create long-term resiliency to minimize our cybersecurity risks?
- What kind of cyber threat information sharing does my business participate in? With whom does my business exchange this information?
- What type of information sharing practices could my business adopt that would help foster community among the different cybersecurity groups where my business is a member?

https://us-cert.cisa.gov/ncas/tips/ST18-007

What can CEOs do to mitigate cybersecurity threats?

The following questions will help CEOs guide discussions about their cybersecurity risk with management:

- What is the threshold for notifying executive leadership about cybersecurity threats?
- What is the current level of cybersecurity risk for our company?
- What is the possible business impact to our company from our current level of cybersecurity risk?
- What is our plan to address identified risks?
- What cybersecurity training is available for our workforce?
- What measures do we employ to mitigate insider threats?
- How does our cybersecurity program apply industry standards and best practices?
- Are our cybersecurity program metrics measureable and meaningful?
- How comprehensive are our cybersecurity incident response plan and our business continuity and disaster recovery plan?
- How often do we exercise our plans?
- Do our plans incorporate the whole company or are they limited to information technology (IT)?
- How prepared is my business to work with federal, state, and local government cyber incident responders and investigators, as well as contract responders and the vendor community?

https://us-cert.cisa.gov/ncas/tips/ST18-007

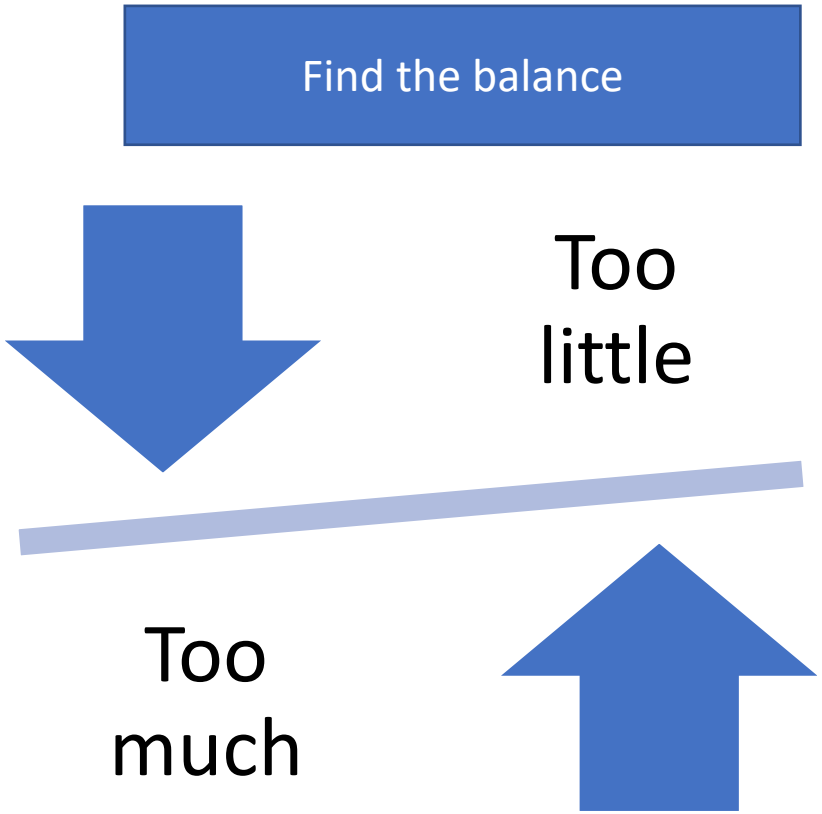
Risks - Identify and Prioritize Information Types

	Example: Customer Contact Information	Info type 1	Info type 2	Info type 3	…
Cost of revelation (Confidentiality)	*Med*				
Cost to verify information (Integrity)	*High*				
Cost of lost access (Availability)	*High.*				
Cost of lost work	*High*				
Fines, penalties, customer notification	*Med*				
Other legal costs	*Low*				
Reputation / public Relations costs	*High*				
Cost to identify and repair problem	*High*				
Overall Score:	*High*				

NIST Publication **NISTIR 7621 Revision 1, Small Business Information Security:** *The Fundamentals* Celia Paulsen Patricia Toth, Table 1, 10 - sample

Budget

- Funding drives all/most activities
  - Personnel
  - Time
  - Equipment
  - Training
  - Resources
  - Upgrades
  - Consultants if required/used
  - Cyber Insurance
- Account for growth, new requirements



Develop Resources – references & SME/S

Image copied from: innovation.ed.gov

Vulnerabilities lead to different paths of attack

Notes by CVSS Environmental Score

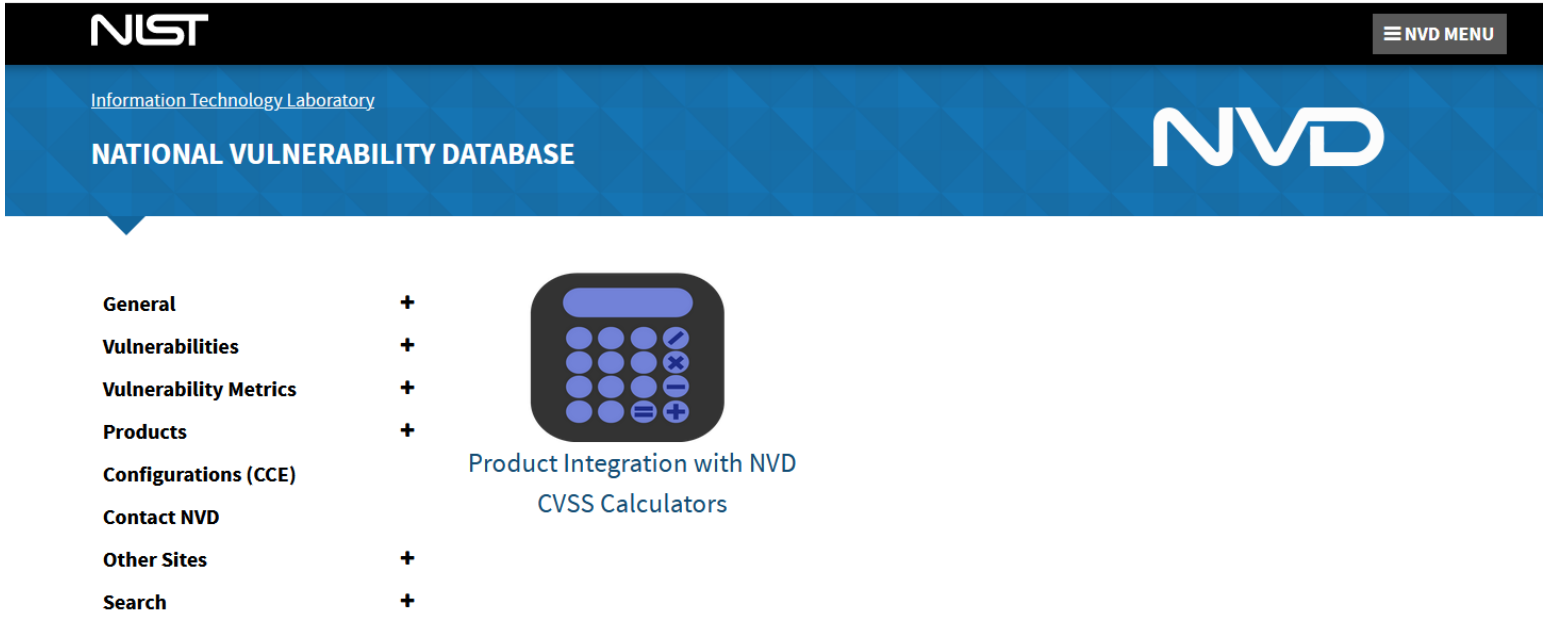
CVSS	Public	ID	Title
9.6	2014-09-24	VU#252743	GNU Bash shell executes commands in exported functions in enviro...
9.5	2014-04-26	VU#222929	Microsoft Internet Explorer CMarkup use-after-free vulnerability
9.5	2014-02-13	VU#732479	Internet Explorer CMarkup use-after-free vulnerability
9.5	2013-01-10	VU#625617	Java 7 fails to restrict access to privileged code
9.5	2012-08-26	VU#636312	Oracle Java JRE 1.7 Expression.execute() and SunToolkit.getField() ...
9.5	2010-08-02	VU#362332	Wind River Systems VxWorks debug service enabled by default
9.5	2010-08-02	VU#840249	Wind River Systems VxWorks weak default hashing algorithm in sta...
9.4	2013-03-04	VU#688246	Oracle Java contains multiple vulnerabilities
9.3	2011-12-27	VU#723755	WiFi Protected Setup (WPS) PIN brute force vulnerability
9.2	2014-08-07	VU#578598	Iridium Pilot and OpenPort contain multiple vulnerabilities
9.0	2014-11-11	VU#505120	Microsoft Secure Channel (Schannel) vulnerable to remote code exe...

https://www.kb.cert.org/vuls/byCVSS visited 9/12/2017

Software

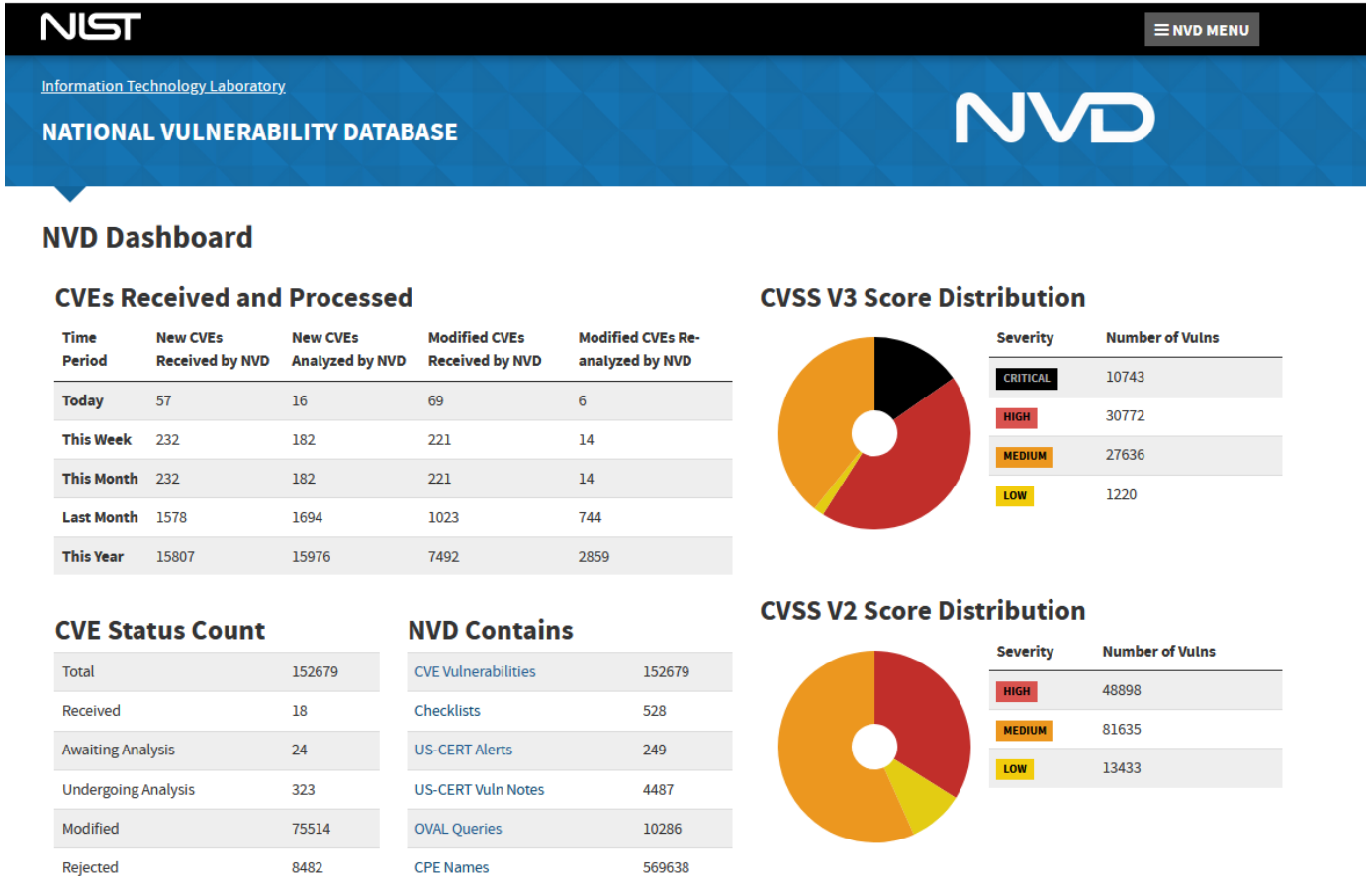
- Identify all systems on/connecting to the network
- Identify owners
- Identify software
- Identify/define – allowed v. rogue software
- Determine patches/security updates/support
- Validate – A/V / Firewall

Identify tools



https://nvd.nist.gov/vuln-metrics/cvss

Resources for awareness & insight



NIST

NVD MENU

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NVD

NVD Dashboard

CVEs Received and Processed

Time Period	New CVEs Received by NVD	New CVEs Analyzed by NVD	Modified CVEs Received by NVD	Modified CVEs Re-analyzed by NVD
Today	57	16	69	6
This Week	232	182	221	14
This Month	232	182	221	14
Last Month	1578	1694	1023	744
This Year	15807	15976	7492	2859

CVSS V3 Score Distribution

Severity	Number of Vulns
CRITICAL	10743
HIGH	30772
MEDIUM	27636
LOW	1220

CVE Status Count

Total	152679
Received	18
Awaiting Analysis	24
Undergoing Analysis	323
Modified	75514
Rejected	8482

NVD Contains

CVE Vulnerabilities	152679
Checklists	528
US-CERT Alerts	249
US-CERT Vuln Notes	4487
OVAL Queries	10286
CPE Names	569638

CVSS V2 Score Distribution

Severity	Number of Vulns
HIGH	48898
MEDIUM	81635
LOW	13433

https://nvd.nist.gov/general/nvd-dashboard

National Vulnerabilities Database

https://nvd.nist.gov/vuln/full-listing

November 2020 entries

Below is a list of CVEs for the selected month.

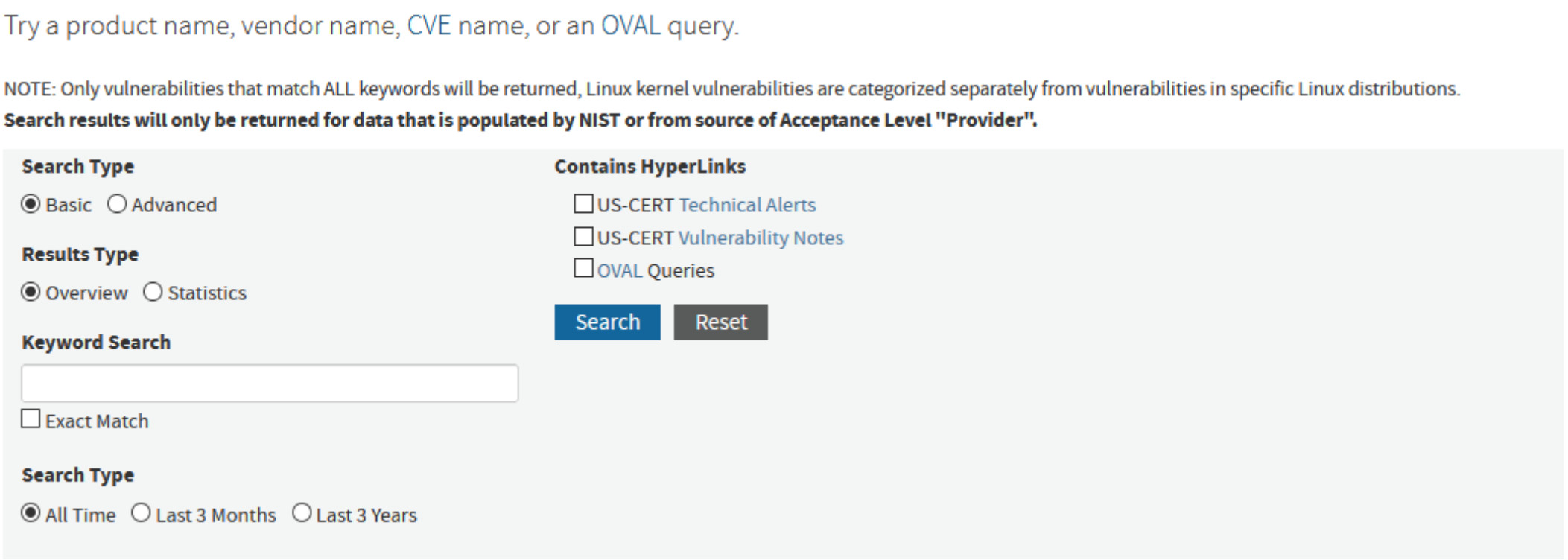
NOTE: The CVEs shown below have a **release date** in the year and month chosen. The CVE ID may show a year value that does not match the release date, however, the release date will fall within the chosen year and month.

466 entries found for November 2020

CVE-2020-25849	CVE-2020-11114	CVE-2020-11125	CVE-2020-11141	CVE-2020-11153	CVE-2020-11154
CVE-2020-11155	CVE-2020-11156	CVE-2020-11157	CVE-2020-11162	CVE-2020-11164	CVE-2020-11169
CVE-2020-11172	CVE-2020-11173	CVE-2020-11174	CVE-2020-3638	CVE-2020-3654	CVE-2020-3657
CVE-2020-3670	CVE-2020-3673	CVE-2020-3678	CVE-2020-3684	CVE-2020-3690	CVE-2020-3692
CVE-2020-3693	CVE-2020-3694	CVE-2020-3696	CVE-2020-3703	CVE-2020-3704	CVE-2018-19950
CVE-2018-19951	CVE-2018-19952	CVE-2018-19954	CVE-2018-19955	CVE-2018-19956	CVE-2018-17932
CVE-2018-19025	CVE-2020-10937	CVE-2020-14425	CVE-2020-14750	CVE-2020-15914	CVE-2020-23639
CVE-2020-24881	CVE-2020-25689	CVE-2020-27358	CVE-2020-27359	CVE-2020-27708	CVE-2020-27982
CVE-2020-27992	CVE-2020-28002	CVE-2020-28030	CVE-2020-28031	CVE-2020-28032	CVE-2020-28033
CVE-2020-28034	CVE-2020-28035	CVE-2020-28036	CVE-2020-28037	CVE-2020-28038	CVE-2020-28039
CVE-2020-28040	CVE-2020-28041	CVE-2020-28042	CVE-2020-28043	CVE-2020-28044	CVE-2020-28045
CVE-2020-28046	CVE-2020-5652	CVE-2020-5653	CVE-2020-5654	CVE-2020-5655	CVE-2020-5656
CVE-2020-5657	CVE-2020-5658	CVE-2020-6014	CVE-2020-8173	CVE-2020-8183	CVE-2020-8236
CVE-2020-9368	CVE-2020-23868	CVE-2020-23989	CVE-2020-26939	CVE-2020-7757	CVE-2020-7758
CVE-2020-9861	CVE-2020-15967	CVE-2020-15968	CVE-2020-15969	CVE-2020-15970	CVE-2020-15971
CVE-2020-15972	CVE-2020-15973	CVE-2020-15974	CVE-2020-15975	CVE-2020-15976	CVE-2020-15977
CVE-2020-15978	CVE-2020-15979	CVE-2020-15980	CVE-2020-15981	CVE-2020-15982	CVE-2020-15983

https://nvd.nist.gov/vuln/full-listing/2020/11

NVD - search



Search Results

Search Parameters:

- Results Type: Overview
- Keyword (text search): python
- Search Type: Search All

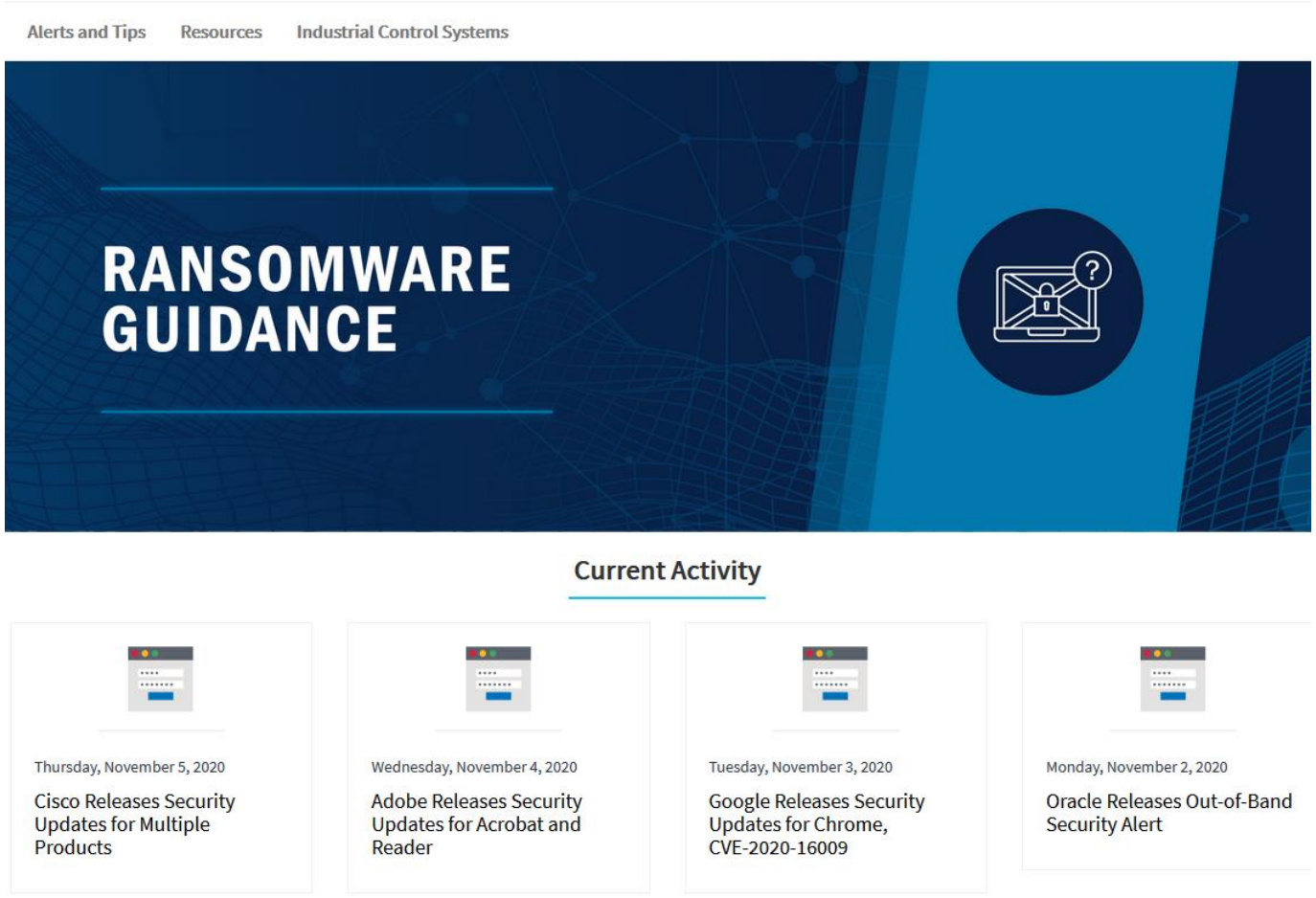
There are **501** matching records.
Displaying matches **1** through **20**.

1 2 3 4 5 6 7 8 9 10 > >>

Vuln ID	Summary	CVSS Severity
CVE-2020-15271	In lookatme (python/pypi package) versions prior to 2.3.0, the package automatically loaded the built-in "terminal" and "file_loader" extensions. Users that use lookatme to render untrusted markdown may have malicious shell commands automatically run on their system. This is fixed in version 2.3.0. As a workaround, the `lookatme/contrib/terminal.py` and `lookatme/contrib/file_loader.py` files may be manually deleted. Additionally, it is always recommended to be aware of what is being rendered with lookatme. **Published:** October 26, 2020; 2:15:14 PM -0400	*V3.x:*(not available) *V2.0:*(not available)
CVE-2020-27619	In Python 3 through 3.9.0, the Lib/test/multibytecodec_support.py CJK codec tests call eval() on content retrieved via HTTP. **Published:** October 21, 2020; 11:16:31 PM -0400	*V3.1:* 9.8 CRITICAL *V2.0:* 7.5 HIGH
CVE-2020-16977	A remote code execution vulnerability exists in Visual Studio Code when the Python extension loads a Jupyter notebook file, aka 'Visual Studio Code Python Extension Remote Code Execution Vulnerability'. **Published:** October 16, 2020; 7:15:17 PM -0400	*V3.1:* 7.8 HIGH *V2.0:* 9.3 HIGH
CVE-2020-4636	IBM Resilient OnPrem 38.2 could allow a privileged user to inject malicious commands through Python3 scripting. IBM X-Force ID: 185503. **Published:** October 16, 2020; 1:15:13 PM -0400	*V3.1:* 7.2 HIGH *V2.0:* 6.5 MEDIUM
CVE-2020-26943	An issue was discovered in OpenStack blazar-dashboard before 1.3.1, 2.0.0, and 3.0.0. A user allowed to access the Blazar dashboard in Horizon may trigger code execution on the Horizon host as the user the Horizon service runs under (because the Python eval function is used). This may result in Horizon host unauthorized access and further compromise of the Horizon service. All setups using the Horizon dashboard with the blazar-dashboard plugin are affected. **Published:** October 16, 2020; 2:15:12 AM -0400	*V3.1:* 9.9 CRITICAL *V2.0:* 9.0 HIGH

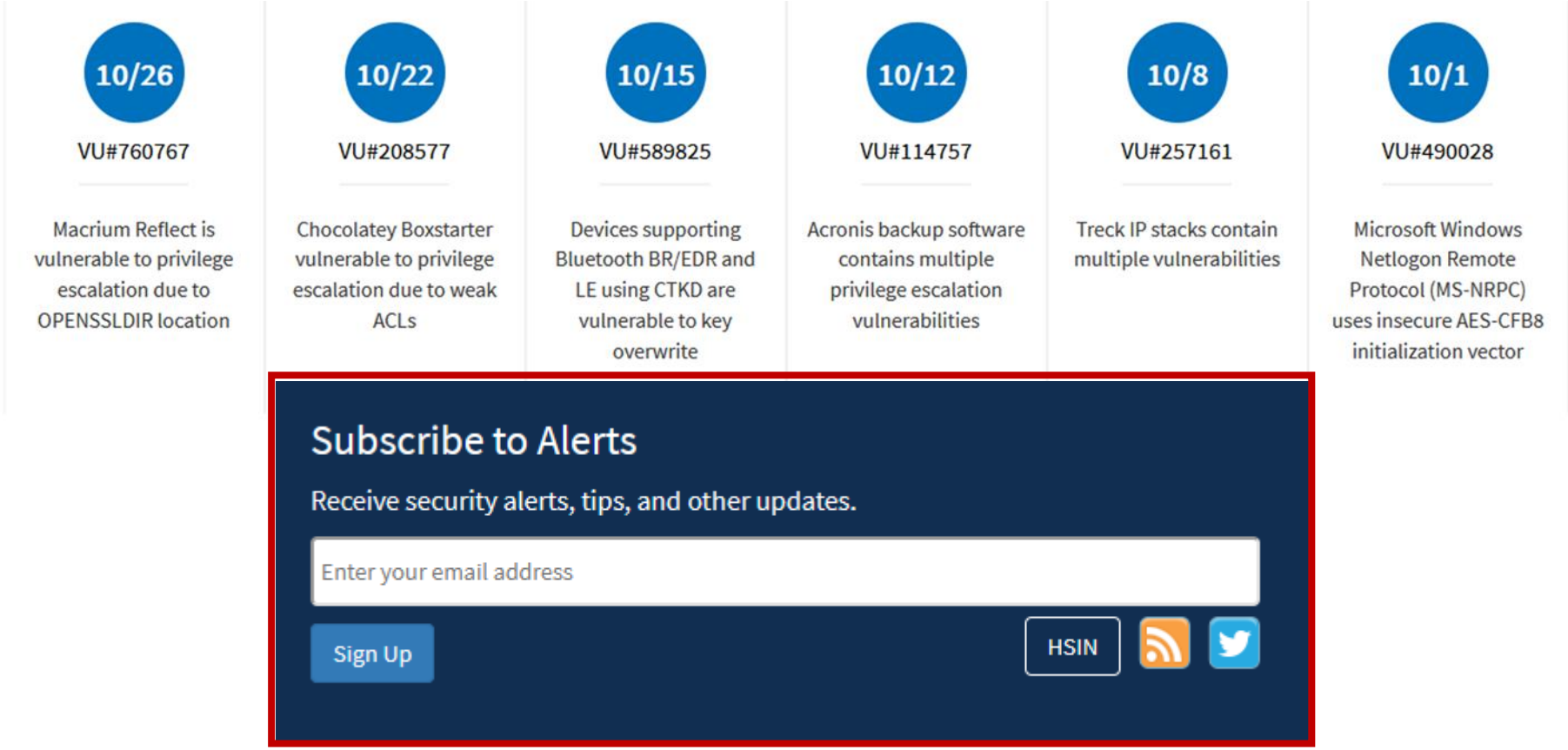
https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=python&search_type=all

Assemble Public and Private resources



https://us-cert.cisa.gov/

Look for and Subscribe – create mail rules



https://us-cert.cisa.gov/

Information Sharing and Analysis Centers

national council of ISACs

HOME | ABOUT NCI | ABOUT ISACS | MEMBER ISACS | EVENTS | PUBLICATIONS | NEWS | CONTACT

ABOUT ISACs

Information Sharing and Analysis Centers (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.

The concept of ISACs was introduced and promulgated pursuant to Presidential Decision Directive-63 (PDD-63), signed May 22, 1998, after which the federal government asked each critical infrastructure sector to establish sector-specific organizations to share information about threats and vulnerabilities. Some ISACs formed as early as 1999, and most have been in existence for at least ten years.

ISACs are trusted entities established by critical infrastructure owners and operators to foster information sharing and best practices about physical and cyber threats and mitigation. Typically nonprofit organizations, ISACs reach deep into their sectors, communicating critical information far and wide and maintaining sector-wide situational awareness.

Most ISACs have 24/7 threat warning and incident reporting capabilities, and may also set the threat level for their sectors. And many ISACs have a track record of responding to and sharing actionable and relevant information more quickly than government partners.

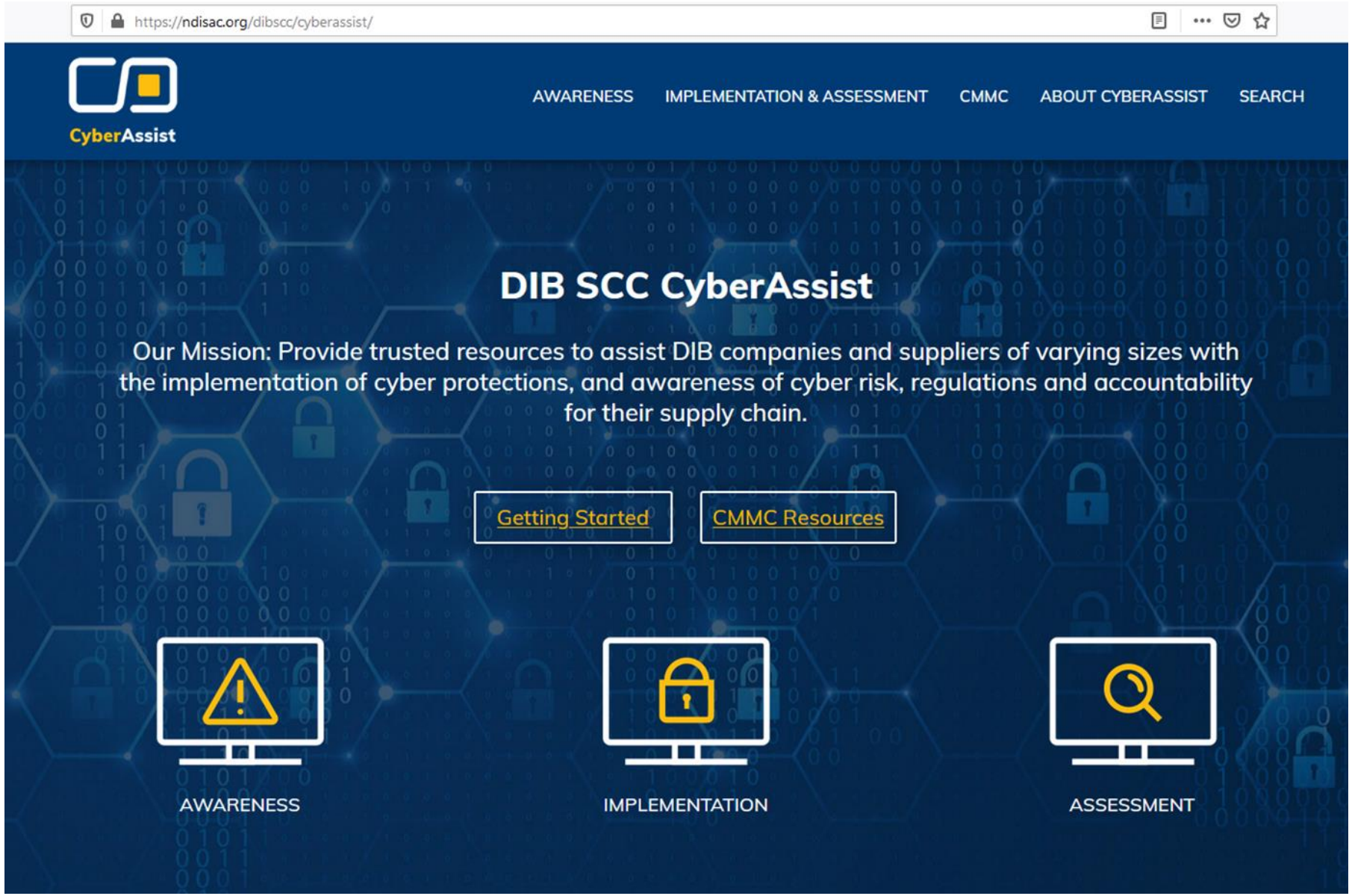
Multi-State ISAC

The mission of the MS-ISAC is to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery.

See Our FAQ → **Read the MS-ISAC Mission & Charter →**

Services Included with Membership

• 24/7 Security Operation Center	• Weekly Top Malicious Domains/IP Report
• Incident Response Services	• Monthly Members-only Webcasts
• Cybersecurity Advisories and Notifications	• Access to Cybersecurity Table-top Exercises
• Access to Secure Portals for Communication and Document Sharing	• Vulnerability Management Program (VMP)
• Cyber Alert Map	• Nationwide Cyber Security Review (NCSR)
• Malicious Code Analysis Platform (MCAP)	• Awareness and Education Materials



https://ndisac.org/dibscc/cyberassist/

DIB SCC Task Force Working Group Top 10 high value controls

Administrative Rights and Privileges

Anti-virus/Malware

Default Passwords

DNS Mitigations

Email Filtering

Employee Training and Awareness

Multi-Factor Authentication

Patching

Perimeter Hardening

Web Content Filtering

https://ndisac.org/dibscc/implementation-and-assessment/top-10-high-value-controls/

DIB SCC Task Force Working Group Top 10 high value controls

Implementation	Assessment

- Boston University – Identity and Access Management Policy
  A sample identity and access management policy for Boston University.
- BrightTalk – Anger, Greed and a Few Mistakes: Human Nature and Privileged Accounts Video presented by CyberArk discussing risks with privilege account misuse.
- BrightTalk – Global State of Privileged Account Management Video presented by Thycotic discussing risks and mitigations for privileged accounts.
- BrightTalk – Simply Indispensable Privileged Account Management & Endpoint Security Video presented by Thycotic discussing risks and mitigations for privileged accounts.
- BrightTalk – Target and Eliminate Privileged Account Security Threats Video presented by McAfee and Lieberman Software discussing privileged account management.
- Grande Prairie Regional College – IT Access Control and User Access Management Policy
  A sample user access management policy for the Grande Prairie Regional College.

https://ndisac.org/dibscc/implementation-and-assessment/top-10-high-value-controls/administrative-rights-and-privileges/

Don’t recreate the wheel or pay if not needed

NIST SP 800-171 Security Controls

Here you will find public resources we have collected on the key NIST SP 800-171 security controls in an effort to assist our suppliers in their implementation of the controls. Select a control family below to display the collected resources for controls within that particular family. Resources include guides, sample policy & procedures, videos, example tools, additional lessons learned, and vendor documentation. In time, resources will be made available that address additional security controls. You will want to check back periodically for updates to this information.

If you wish to provide any feedback about the resources, please click here.

3.1 Access Control	3.2 Awareness and Training	3.3 Audit and Accountability	3.4 Configuration Management	3.5 Identification and Authentication	3.6 Incident Response	3.7 Maintenance	3.8 Media Protection
	3.9 Personnel Security	3.10 Physical Protection	3.11 Risk Assessmen	3.12 Security Assessment	3.13 Systems and Communications Protection	3.14 Systems and Information Integrity	

Northrop Grumman / Suppliers - OASIS / **NIST SP 800-171 Security Controls**

https://www2.northropgrumman.com/suppliers/Pages/CybersecurityControlsLanding.aspx

3.4 Configuration Management – for example

3.4.1 Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems.

Guides

- DISA Security Technical Implementation Guides (STIGS)
- NIST Computer Resource Center National Checklist Program Repository
- Microsoft TechNet – Geek of All Trades: Automate Baseline Security

Sample Policy & Procedures

- SANS Institute - Sample Server Policy
- SANS Institute - Sample Router and Switch Policy
- Berkeley Information Security and Policy – Secure Device Configuration Guideline

Videos

- BrightTALK - Security Configuration Management - The Keys to the Digital Kingdom

Example Tools

- Microsoft Security Compliance Manager
- Tenable Security Center
- NIST - SCAP Intro
- OSCAP
- Linux SCAP Workbench
- Center for Internet Security - Benchmarks

Additional Lessons Learned

- Center for Internet Security – Top 20 Security Controls

Vendor Documentation

- Cisco Security Baseline Checklist

Identify/explore a variety of resources – then select

CUI Training

The CUI Executive Agent develops training modules for the CUI Program, designed for a widespread audience at multiple levels within the government and beyond. The modules below can be used to supplement any training or awareness efforts by Executive branch entities or other stakeholders (i.e., Nonfederal organizations).

Select a subject from the list below to transfer directly to training modules for that topic:

- Controlled Environments
- CUI Program Overview
- Decontrolling
- Destruction
- Freedom of Information Act (FOIA)
- Lawful Government Purpose
- Introduction to Marking
- Marking Non-Traditional Documents
- Marking Commingled Information
- Unauthorized Disclosures: Preventing and Reporting
- CUI Briefing January 27, 2017

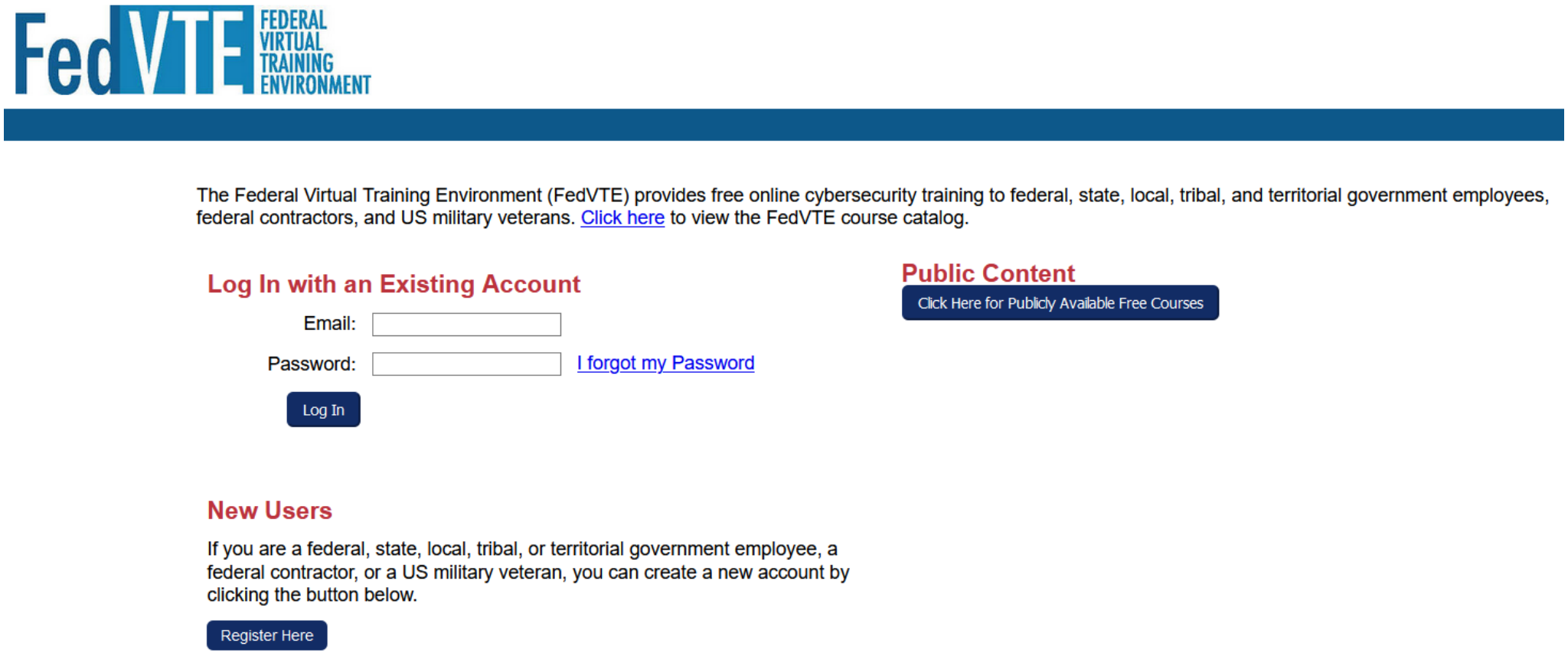
https://www.archives.gov/cui/training.html

Know the Risk Raise Your Shield

The National Counterintelligence and Security Center

https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-know-the-risk-raise-your-shield

Take advantage of free & credible resources



Courses available to the public

Public Courses

No login required

The Federal Virtual Training Environment (FedVTE) provides the following courses free of charge and without login requirements. You must use a modern browser (Edge, Chrome, Firefox) and have cookies enabled to track your progress in these courses.

Refer to the FAQ for more questions and answers on Public FedVTE

Publicly Available Free Courses

101 Coding for the Public

101 Critical Infrastructure Protection for the Public

Cryptocurrency for Law Enforcement for the Public

Cyber Supply Chain Risk Management for the Public

101 Reverse Engineering for the Public

Fundamentals of Cyber Risk Management

Don't Wake Up to a Ransomware Attack - 1 Hour

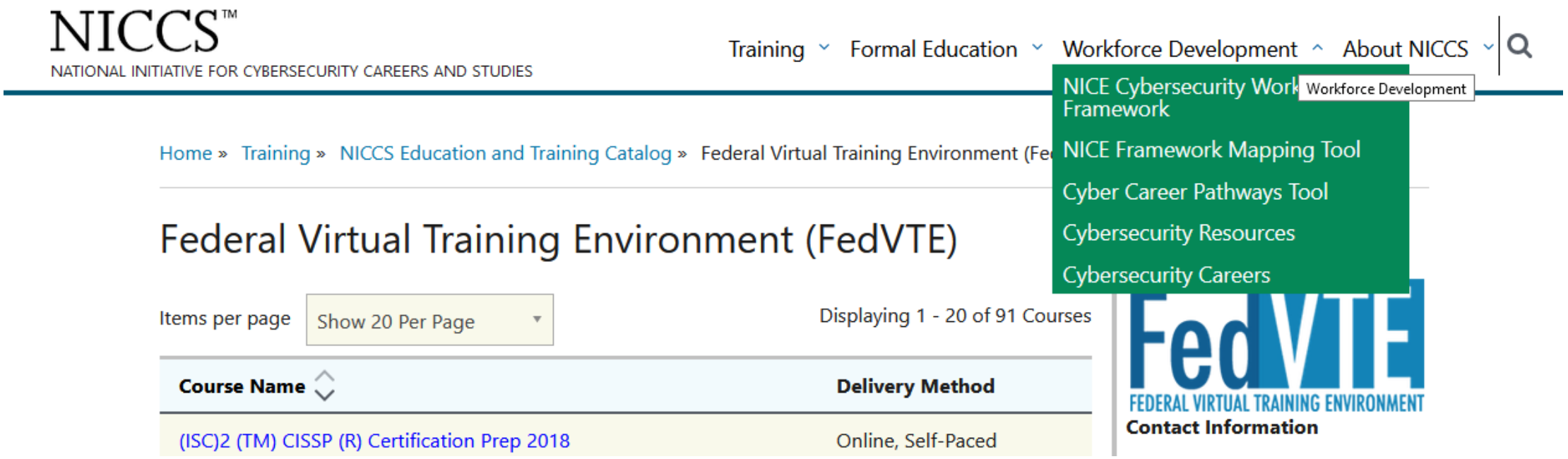
Introduction to Cyber Intelligence - 2 Hours

Don't Get Caught in the Storm - Protecting Your Cloud Assets - 1 Hour

Cyberessentials - 1 Hour

https://fedvte.usalearning.gov/public_fedvte.php

Resources for skill development & workforce



https://niccs.cisa.gov/training/search/federal-virtual-training-environment-fedvte

NCSC Awareness Materials

- Social Media Deception
- Social Engineering
- Spear phishing 2017
- Spear Phishing (30 second trailer)
- Spear Phishing Full Video
- Social Media Deception Trailer
- Social Media Deception Full Video
- Travel Awareness
- Human Targeting
- Supply Chain Risk Management
- Economic Espionage

Internet Storm Center - Ports

by Reports

Port	Reports
22	159815
2222	59050
445	38593
25	36460
23	28765
443	20471
80	15615
6881	14068
53	13755
3389	7781

by Targets

Port	Targets
22	1360
23	1265
80	854
445	771
8080	764
1433	518
443	435
5555	405
81	384
25	380

by Sources

Port	Sources
445	10811
23	5585
22	4605
1433	3324
80	2905
2222	2497
6881	2476
8080	1928
55361	1331
443	1068

View Port Report Page

https://www.dshield.org/top10.html

Internet Storm Center – Top 10 IP Addresses

IP Address	Reports	Target IPs	First Seen	Last Seen
146.088.240.004 (US)	258,396	3,606	2020-08-10	2020-11-06
195.054.161.122 (RU)	323,802	3,520	2020-08-07	2020-11-06
087.251.074.018 (RU)	264,283	3,460	2020-09-04	2020-11-06
045.129.033.129 (DE)	439,017	3,451	2020-09-17	2020-11-06
045.129.033.084 (DE)	411,349	3,449	2020-09-03	2020-11-06
045.093.201.115 (RU)	104,473	3,077	2020-10-18	2020-11-06
045.146.164.085 (RU)	135,977	3,040	2020-10-13	2020-11-06
045.129.033.004 (DE)	162,892	2,416	2020-07-21	2020-11-05
045.129.033.044 (DE)	55,367	2,234	2020-10-16	2020-11-06
005.188.086.206 (RU)	204,729	2,179	2020-10-31	2020-11-05

View Top Sources Page

Useful InfoSec Links

- Internet Status – 25
- Malware Information – 16
- Security Dashboards – 8
- Security News – 20
- Security Blogs – 38
- Vendor Security Advisories - 14

Security News

- The Register ____ [vote in favor|against]
- Threatpost Kaspersky ____ [vote in favor|against]
- Heise Security ____ [vote in favor|against]
- Computerworld Security News ____ [vote in favor|against]
- SecurityNewsPortal ____ [vote in favor|against]
- Info Security News ____ [vote in favor|against]
- Security Week ____ [vote in favor|against]
- Wired Threat Level ____ [vote in favor|against]
- Common Vulnerability Enumeration CVE ____ [vote in favor|against]
- MU Online Cybersecurity News ____ [vote in favor|against]
- Infosecurity ____ [vote in favor|against]
- InfoSec News Information Security Cybersecurity News ____ [vote in favor|against]
- Risky Business Podcast and weekly newsletter Category Podcast ____ [vote in favor|against]
- Cyberscoop ____ [vote in favor|against]
- Network World Security Research Center ____ [vote in favor|against]
- commissum ____ [vote in favor|against]
- CyberSoftcom ____ [vote in favor|against]
- IT Security Jobs ____ [vote in favor|against]
- Computer Security blog ____ [vote in favor|against]
- Cybersecuritycentral ____ [vote in favor|against]

Security Blogs

- Krebs on Security ____ [vote in favor|against]
- SANS Forensics ____ [vote in favor|against]
- Schneier on Security ____ [vote in favor|against]

https://www.dshield.org/links.html

SANS Reading Room

Latest 25 Papers Added to the Reading Room

Threat Intelligence Solutions: A SANS Review of Anomali ThreatStream
Analyst Paper (requires membership in SANS.org community)
by TJ Banasik - November 2, 2020 in Intrusion Detection, Threats/Vulnerabilities

- **Associated Webcasts:** Threat Intelligence Solutions: A SANS Review of Anomali ThreatStream
- **Sponsored By:** Anomali

+ Overview
Login
Join SANS.org

How to Create a Scalable and Automated Edge Strategy in the AWS Cloud
Analyst Paper (requires membership in SANS.org community)
by Dave Shackleford - October 30, 2020 in Best Practices, Cloud Security

- **Associated Webcasts:** How to Create a Scalable and Automated Edge Strategy in the AWS Cloud
- **Sponsored By:** AWS Marketplace

+ Overview
Login
Join SANS.org

Fear of the Unknown: A Metanalysis of Insecure Object Deserialization Vulnerabilities
by Karim Lalji - October 28, 2020 in Penetration Testing

+ Overview
Download

Verifying Universal Windows Platform (UWP) Signatures at Scale
SANS.edu Graduate Student Research
by Joal Mendonsa - October 28, 2020 in Intrusion Detection, Incident Handling, Microsoft Windows, Threat Hunting

+ Overview
Download

https://www.sans.org/reading-room/

Response assistance & Resources

https://www.first.org/

FIRST Teams

This is a list of the contact information for incident response teams participating in FIRST, the Forum of Incident Response and Security Teams. The teams are responsible for providing FIRST with their latest contact information for this page. The list is alphabetized by team name. All telephone numbers are preceded with the appropriate country code.

Team contact information provided for Incident Response purposes only. FIRST strictly prohibits the use of contact information for solicitation or marketing.

Search FIRST Teams There are 540 Teams.

Team	Official Team Name	Country
AB-CSIRT	Alpha Bank Computer Security Incident Response Team	GR
Accenture	Accenture Cyber Fusion Center	CZ
Access Now Digital Security Helpline	Access Now Digital Security Helpline	CR
ACKCERT	Ackcent CERT	ES
ACOnet-CERT	ACOnet-CERT	AT
Acuity Brands PSIRT	Acuity Brands Product Security Incident Response Team	US

https://www.first.org/members/teams/

FIRST Team – contact info, eg

Acuity Brands PSIRT

Team Information

Team name	Acuity Brands PSIRT
Official team name	Acuity Brands Product Security Incident Response Team
Member since	August 27, 2018
Host organization	Acuity Technology Group
Country of team	United States of America (the) US
Date of establishment	2018-08-28
Website	https://acuitybrands.com

Team Contact Information

Regular telephone number	6145194715
Emergency telephone number	9198222162
E-mail address	psirt@acuitybrands.com
Postal address	One Lithonia Way Conyers, GA 30012

https://www.first.org/members/teams/acuity_brands_psirt

Log Protection

- logs contain records of system and network security
- they need to be protected from breaches of their confidentiality and integrity
- Improperly securing - intentional and unintentional alteration and destruction
  - May allow malicious activity to go on unnoticed
  - For example, many rootkits are specifically designed to alter logs
- Protect availability of logs – maximum size / overwriting

NIST SP 800-92 Computer Security and Log Management, 2.3.9 page 2-9

Maximizing Log value

- Identify as high priority
  - Combat the notion of boring and of low benefit
- Provide sufficient tools
  - Assists with automation
  - Helps to identify patterns that a human will not see
- Provide training for efficient performance
- Reactive tool
  - After an event

NIST SP 800-92 Computer Security and Log Management, 2.3.3 page 2-10

Categorize information

TLP:GREEN

https://www.first.org/members/teams/acuity_brands_psirt

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
https://www.us-cert.gov/tlp/

MS-ISAC ADVISORY NUMBER: 2020-148 DATE(S) ISSUED: 11/03/2020

Traffic Light Protocol - Definitions

Color	When should it be used?	How may it be shared?
TLP:RED  Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER  Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN  Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE  Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

US-Cert Alerts

National Cyber Awareness System > Alerts

Alerts provide timely information about current security issues, vulnerabilities, and exploits. Sign up to receive these technical alerts in your inbox or subscribe to our RSS feed.

2020 | 2019 | 2018 | 2017 | 2016 | 2015 | 2014 | 2013 | 2012 | 2011 | 2010 | 2009 | 2008 | 2007 | 2006 | 2005 | 2004

AA20-304A : Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data
AA20-302A : Ransomware Activity Targeting the Healthcare and Public Health Sector
AA20-301A : North Korean Advanced Persistent Threat Focus: Kimsuky
AA20-296B : Iranian Advanced Persistent Threat Actors Threaten Election-Related Systems
AA20-296A : Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets
AA20-283A : APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations
AA20-280A : Emotet Malware
AA20-275A : Potential for China Cyber Response to Heightened U.S.–China Tensions
AA20-266A : LokiBot Malware
AA20-259A : Iran-Based Threat Actor Exploits VPN Vulnerabilities
AA20-258A : Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity
AA20-245A : Technical Approaches to Uncovering and Remediating Malicious Activity
AA20-239A : FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks
AA20-227A : Phishing Emails Used to Deploy KONNI Malware
AA20-225A : Malicious Cyber Actor Spoofing COVID-19 Loan Relief Webpage via Phishing Emails
AA20-209A : Potential Legacy Risk from Malware Targeting QNAP NAS Devices

https://us-cert.cisa.gov/ncas/alerts

Develop Resources – be selective

Booz | Allen | Hamilton®

8 CYBER THREAT TRENDS TO WATCH IN 2021

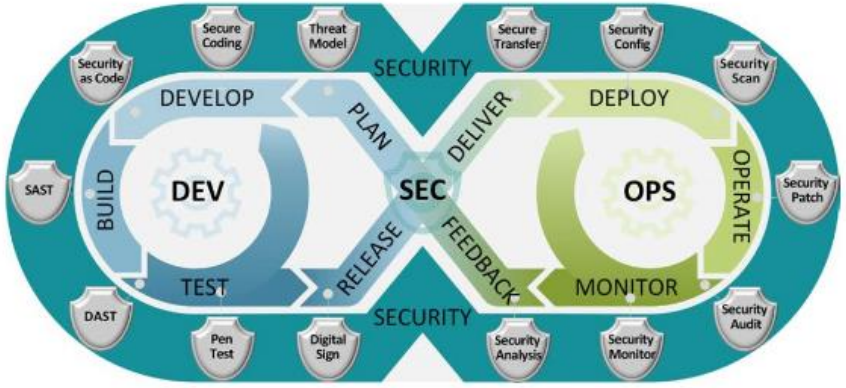
Are you ready for the new and evolving cyber challenges 2021 will bring? Read our **2021 Cyber Threat Trends Outlook** for a glimpse into next year's cyber threat ecosystem and mitigation recommendations that will keep you ahead of your adversaries.

DEVSECOPS

DevSecOps is a set of software development practices that combines software development (Dev), security (Sec), and information technology operations (Ops) to secure the outcome and shorten the development lifecycle.

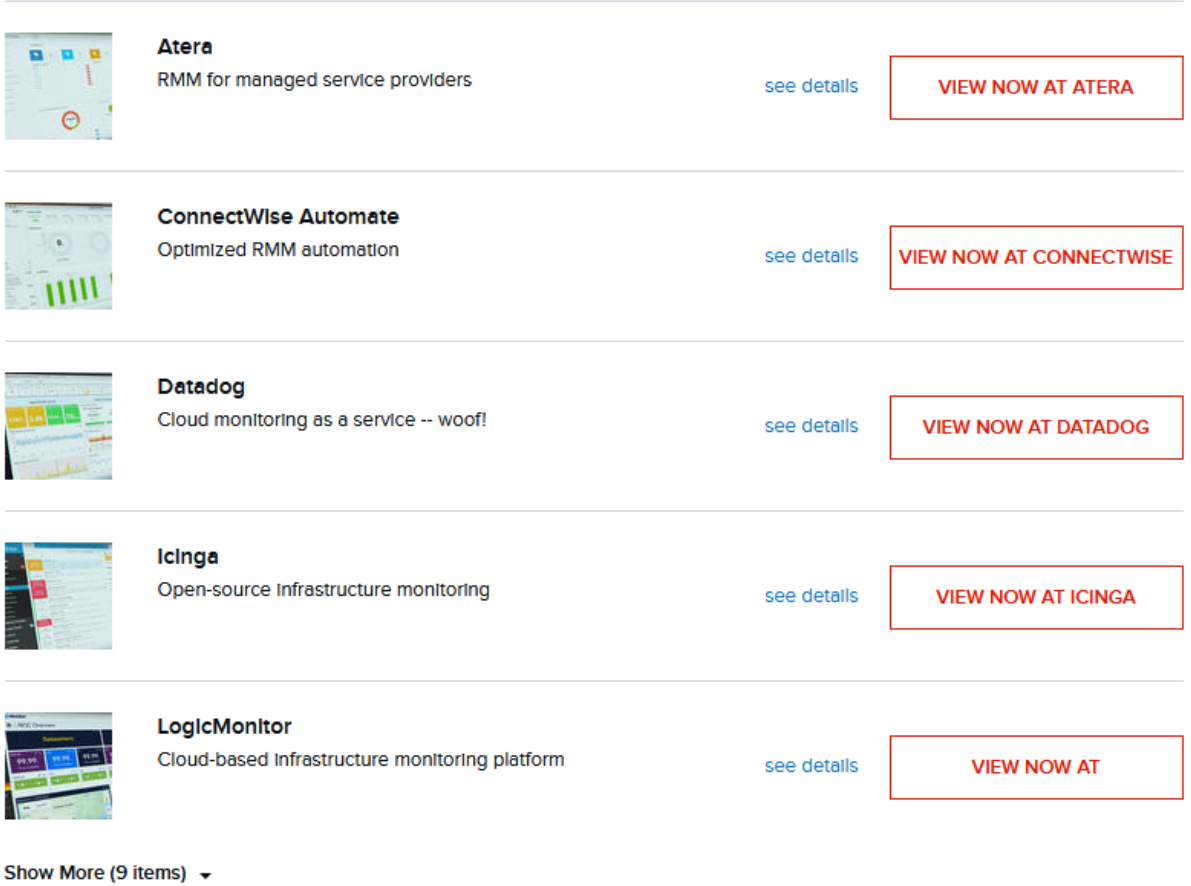
DEVSECOPS MISSION

The DevSecOps Mission is to develop a Continuous Monitoring (CM) approach for all Department of Defense (DoD) mission partners that monitors and provides compliance enforcement of containerized applications which cover all the DevSecOps pillars (Develop, Build, Test, Release & Deploy, and Runtime) for a secure posture with the focus being on automation and integration going forward.



https://public.cyber.mil/devsecops/

Best network monitoring tools in 2020



https://www.zdnet.com/article/best-network-monitoring-tools/

UPCOMING TRAINING - EVENTS

ACQUISITION HOUR LIVE WEBINAR SERIES

- November 17, 2020

  Changes, Delays and Disputes in Federal Construction Contracts
  CLICK HERE for additional information
  Presented by Helen Henningsen, Wisconsin Procurement Institute

- January 20, 2020

  Acquisition Hour: beta.SAM.gov - An Update and Overview
  CLICK HERE for additional information
  Presented by Kim Garber, Wisconsin Procurement Institute

CYBER FRIDAY LIVE WEBINAR SERIES

Sept 11, 2020	A Deep Dive into DFARS 252.204-7012 - Looking beyond NIST 800-171 r1
Sept 25, 2020	Information Security - An overview of programs, general requirements and resources
Oct 9, 2020	Economic Espionage - You have what they want.
Oct 23, 2020	Guarding and Securing Intangibles - Protecting what you cannot see and touch
Nov 6, 2020	Tools, practices and resources for your cyber-security toolbox
Nov 20, 2020	An overview of cyber-threats - What you can't see - can put you out of business!
Dec 4, 2020	Securing the Supply Chain - "No man is an island"
Dec 18, 2020	Developing and implementing practices, policies and procedures using CMMC reference documents
Jan 8, 2021	The other side of CMMC
Jan 22, 2021	Overview of CMMC Level 1
Feb 5, 2021	Embarking on the path to CMMC Level 3
Feb 19, 2021	Preparing for a CMMC Certification assessment
Mar 5, 2021	CMMC Level 3 - Completing the steps needed to protect Controlled Unclassified Information.

PRESENTED BY

WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

TECHNOLOGY INNOVATION CENTER at Research Park

NCMA National Contract Management Association
WISCONSIN

11/6/20

- SAVE THE DATE-

MARKETPLACE WISCONSIN

December 8-10, 2020

The first virtual marketplace will connect statewide business owners looking to do business with state, federal and local governments, as well as the private sector, in a virtual format over the course of a week.

More info at https://www.wispro.org/event/marketplace-2020-virtual/

TCA The Contracting Academy

Developing and Growing Government Contractors

December 8-10, 2020

The Contracting Academy is an opportunity for businesses to grow their technical knowledge of contracting with the State of Wisconsin, Federal Government and Government Prime contractors. This series of workshops will benefit established businesses looking to grow and develop their government sales.

More info at https://www.wispro.org/event/the-contracting-academy-virtual/

WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

A CRITICAL NOTICE FROM WPI

- If you are a current **FEDERAL / DOD CONTRACTOR or SUBCONTRACTOR** – you may have **CYBER – DATA SECURITY REQUIREMENTS** in your contract.
- If you are responding to any **CURRENT FEDERAL SOLICITATIONS** - be aware of your obligations:
  - Key clauses are 52.204-21, 252.204-7008 and 252.204-7012
  - Review for other possible requirements
- If you are a **DOD CONTRACTOR or SUBCONTRACTOR** – you will have new **CYBER COMPLIANCE – CERTIFICATION REQUIREMENTS** that may impact your business as early as the end of this calendar year.
  - See: https://www.acq.osd.mil/cmmc and https://www.cmmcab.org for more up to date information.
  - *Contact Marc Violante at WPI - marcv@wispro.org or 920-456-9990*

CONTINUING PROFESSIONAL EDUCATION

CPE Certificate available, please contact:

Benjamin Blanc

benjaminb@wispro.org

PRESENTED BY

Wisconsin Procurement Institute (WPI)
www.wispro.org

Marc Violante
Wisconsin Procurement Institute (WPI)
marcv@wispro.org | 920-456-9990

10437 Innovation Drive, Suite 320
Milwaukee, WI 53226