Wisconsin Procurement Institute

An APEX Accelerator

Cyber Friday:

Building a CMMC Program: 3.1.2 Security Awareness Training, Role-Based Training, and Insider Threat Training

June21 | 11:00 am - Noon

Presented by:

Matt Frost, Wisconsin Procurement Institute

NCMA NATIONAL CONTRACT MANAGEMENT ASSOCIATION WISCONSIN

Webinar Etiquette

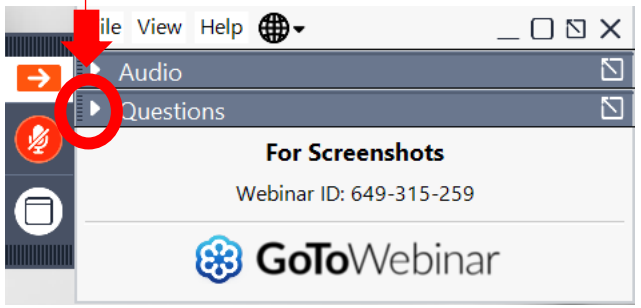
PLEASE

- Log into the GoToWebinar session with the name that you registered with online
- Place your phone or computer on MUTE
- Use the QUESTIONS option to ask your question(s).
  - We will share the questions with our guest speaker who will respond to the group

THANK YOU!

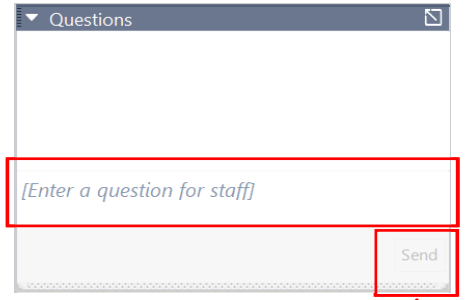
OPENING THE QUESTIONS BOX

Click here to access within the Control Panel



USING THE QUESTIONS BOX

Type questions here at any time during a presentation



Click Send when ready to submit a question

Wisconsin Procurement Institute

An APEX Accelerator

Assisting Wisconsin businesses compete in the government marketplace.

WPI is Wisconsin's APEX ACCELERATOR

The APEX Accelerators program, under management of the Department of Defense (DOD) Office of Small Business Programs (OSBP), plays a critical role in the Department's efforts to identify and engage with a wide range of businesses entering and participating in the defense supply-chain. The program provides the education and training that all businesses need to participate to become capable of participating in DOD and other government contracts.

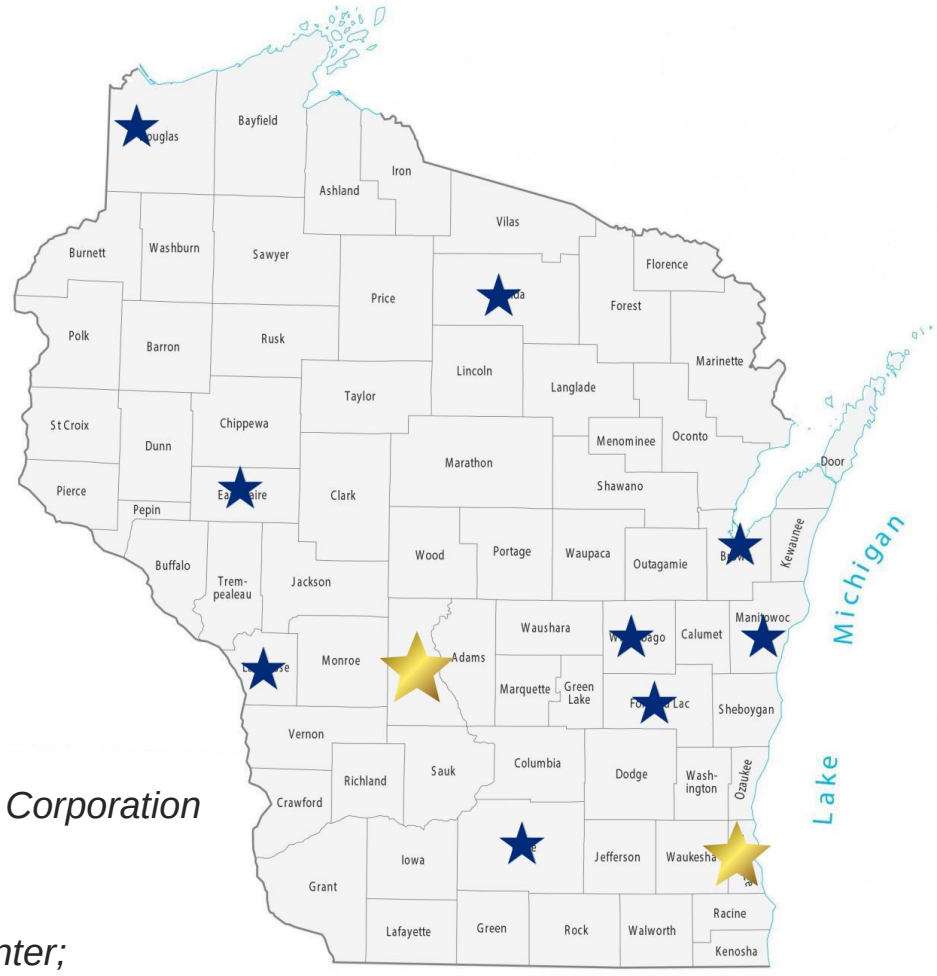
WPI provides services to all of Wisconsin's 72 counties

- Individual counseling at our offices, client's facility or virtually
- Small group training – webinars and workshops
- Conferences including one on one buyer meetings – Marketplace, The Contracting Academy, Small Business Academy, Wisconsin Federal Contractor Forum, Acquisition Hour, Cyber Fridays, DOD Roadmap series, Government Opportunities Business Conference, End of Year Federal Contractor Update, Annual DOD Contract Management Update, Evening FAR sessions and more……

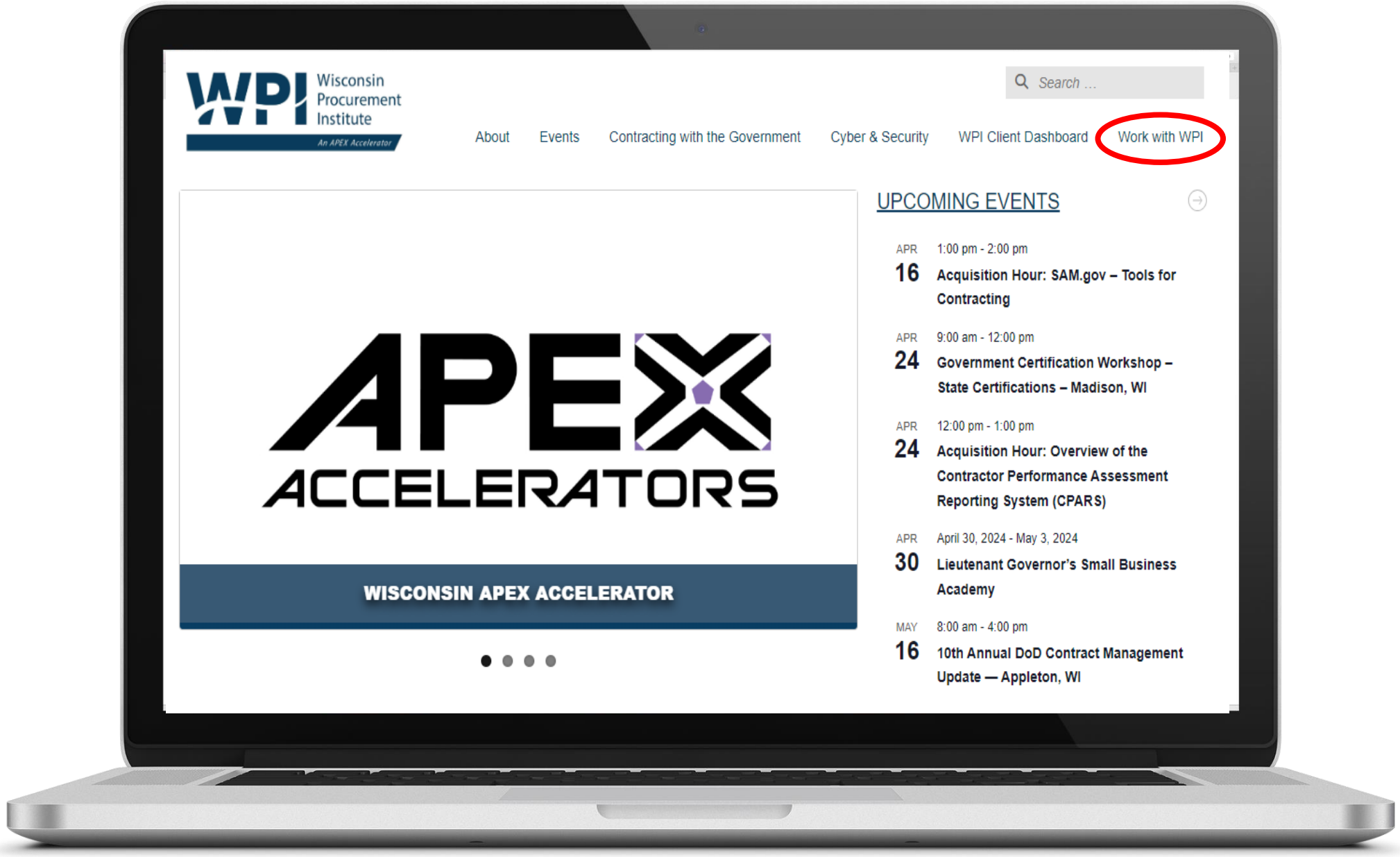
www.wispro.org

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)*
- **EAU CLAIRE**
  - *Western Dairyland*
- **FOND DU LAC**
  - *Envision Greater Fond du Lac*
- **GREEN BAY**
  - *NWTC Startup Hub*
- **LACROSSE**
  - *Veterans in Professions*
- **MANITOWOC**
  - *Progress Lakeshore*
- **OSHKOSH**
  - *Greater Oshkosh Economic Development Corporation*
- **SUPERIOR**
  - *Small Business Dev Center; UW Superior*



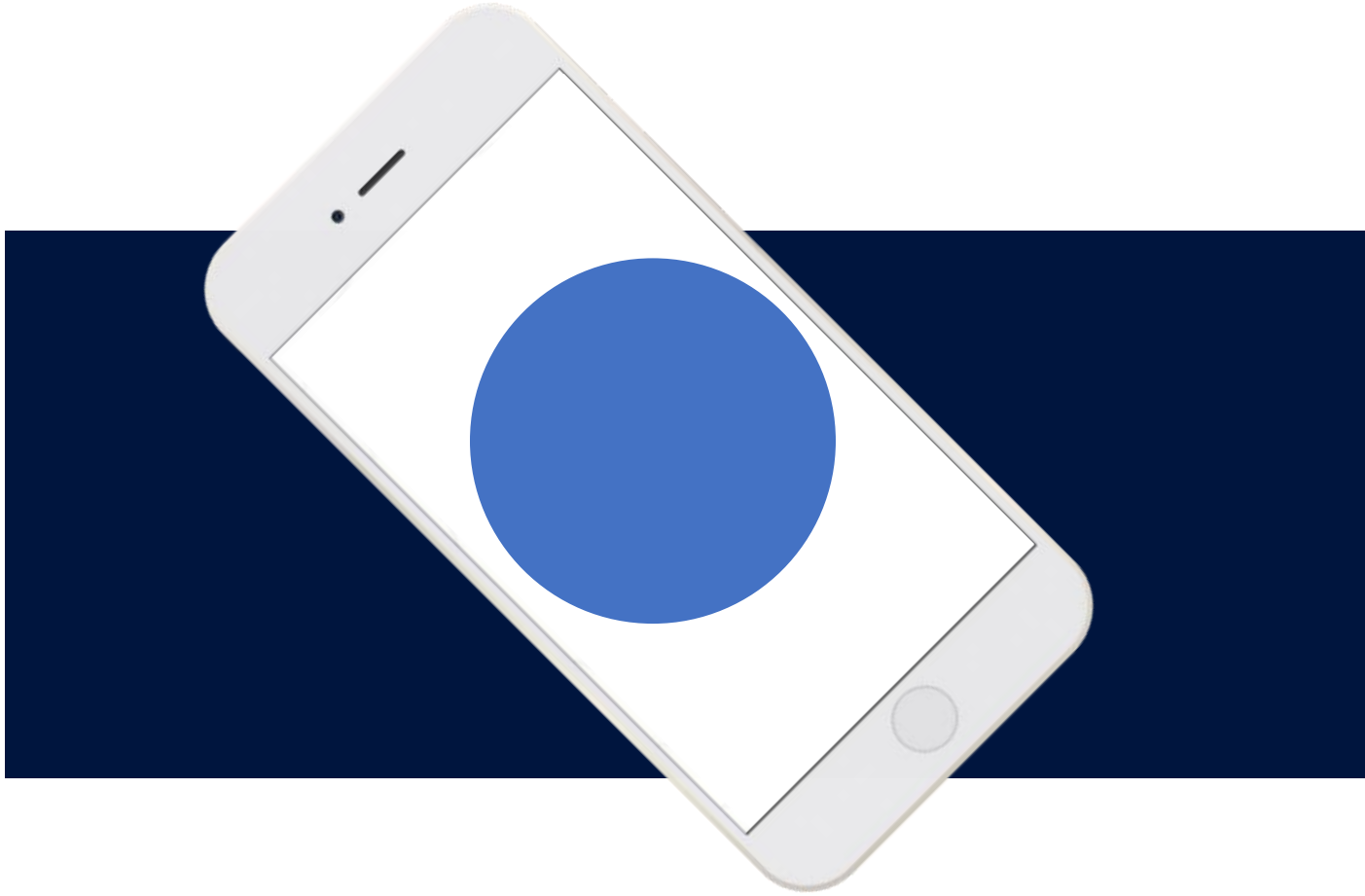
Wisconsin Procurement Institute
An APEX Accelerator


WPI Wisconsin Procurement Institute
An APEX Accelerator
Search ...
About
Events
Contracting with the Government
Cyber & Security
WPI Client Dashboard
Work with WPI
APEX ACCELERATORS
WISCONSIN APEX ACCELERATOR
UPCOMING EVENTS
APR 16 1:00 pm - 2:00 pm
Acquisition Hour: SAM.gov – Tools for Contracting
APR 24 9:00 am - 12:00 pm
Government Certification Workshop – State Certifications – Madison, WI
APR 24 12:00 pm - 1:00 pm
Acquisition Hour: Overview of the Contractor Performance Assessment Reporting System (CPARS)
APR 30 April 30, 2024 - May 3, 2024
Lieutenant Governor's Small Business Academy
MAY 16 8:00 am - 4:00 pm
10th Annual DoD Contract Management Update — Appleton, WI

Documentation for NIST SP 800-171r2 Controls

Wisconsin Procurement Institute

AN APEX ACCELERATOR



CYBER FRIDAY SESSIONS – May 17th, 2024

DFARS 252.204-7012

National Institute of Standards and Technology

The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017.

The Contractor shall notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement.

When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract… the Contractor shall rapidly report cyber incidents to DoD.

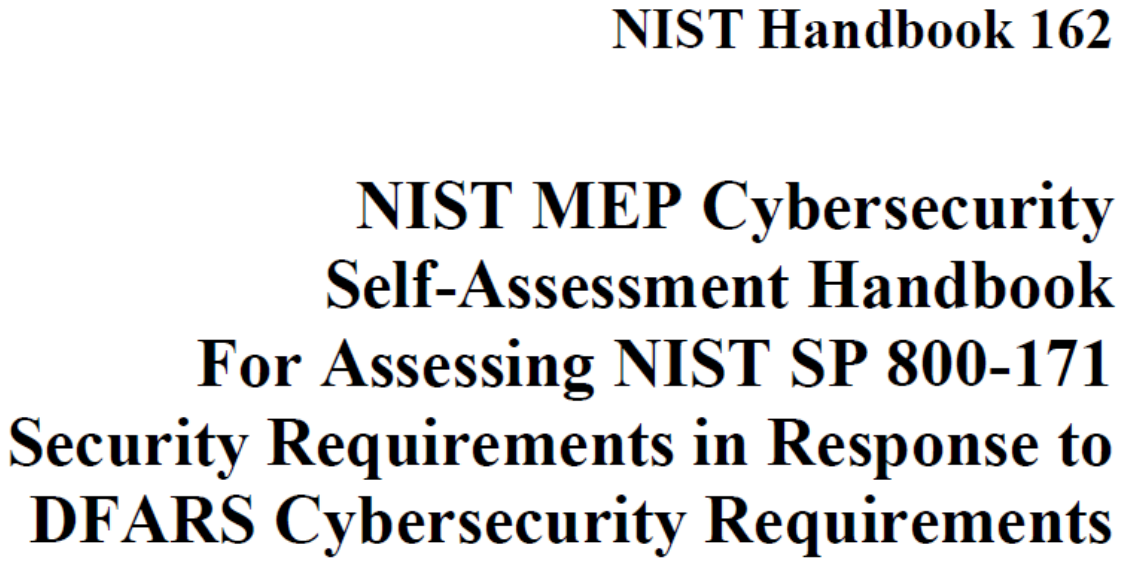
DFARS 252.204-7021

The Cybersecurity Maturity Model Certification (CMMC) is a framework that measures a contractor's cybersecurity maturity to include the implementation of cybersecurity practices…

(b) Requirements. The Contractor shall have a current (i.e. not older than 3 years) CMMC certificate at the CMMC level required by this contract and maintain the CMMC certificate at the required level for the duration of the contract.

14 Families – 110 Controls – 320 Audit Objectives

- Access Control
- **Awareness and Training**
- Audit and Accountability
- Configuration Management
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Risk Assessment
- Security Assessment
- System and Communications Protection
- System and Information Integrity



1 NIST Handbook 162

NIST MEP Cybersecurity Self-Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements

2 NIST SP 800-171A

NIST Special Publication 800-171A
Assessing Security Requirements for Controlled Unclassified Information

3 NIST SP 800-18r1

NIST Special Publication 800-18
Revision 1
Guide for Developing Security Plans for Federal Information Systems

Reading the Controls

NIST SP 800-171

1

Security Awareness and Training Policy

2

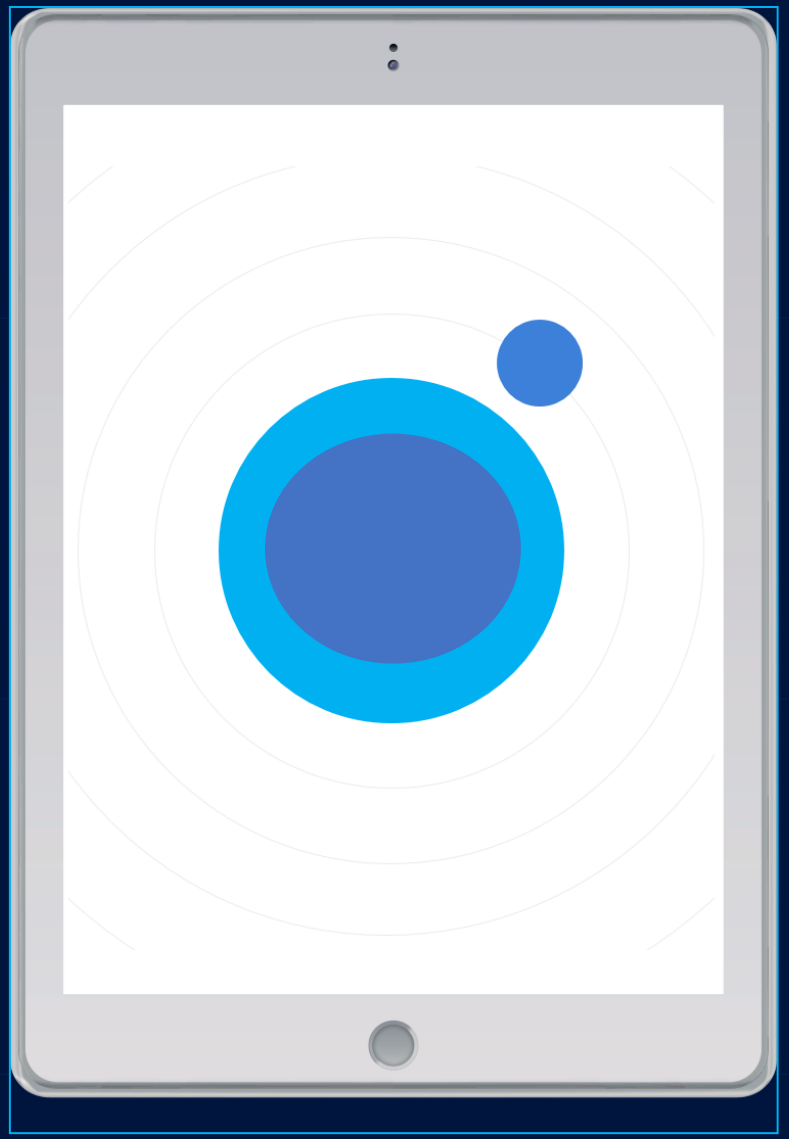
The 3 Trainings

3

Maintaining a Record

3.2.1	SECURITY REQUIREMENT Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.2.1[a] *security risks associated with organizational activities involving CUI are identified.*
	3.2.1[b] *policies, standards, and procedures related to the security of the system are identified.*
	3.2.1[c] *managers, systems administrators, and users of the system are made aware of the security risks associated with their activities.*
	3.2.1[d] *managers, systems administrators, and users of the system are made aware of the applicable policies, standards, and procedures related to the security of the system.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Security awareness and training policy; procedures addressing security awareness training implementation; relevant codes of federal regulations; security awareness training curriculum; security awareness training materials; system security plan; training records; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with responsibilities for security awareness training; personnel with information security responsibilities; personnel composing the general system user community; personnel with responsibilities for role-based awareness training]. Test: [*SELECT FROM:* Mechanisms managing security awareness training; mechanisms managing role-based security training].

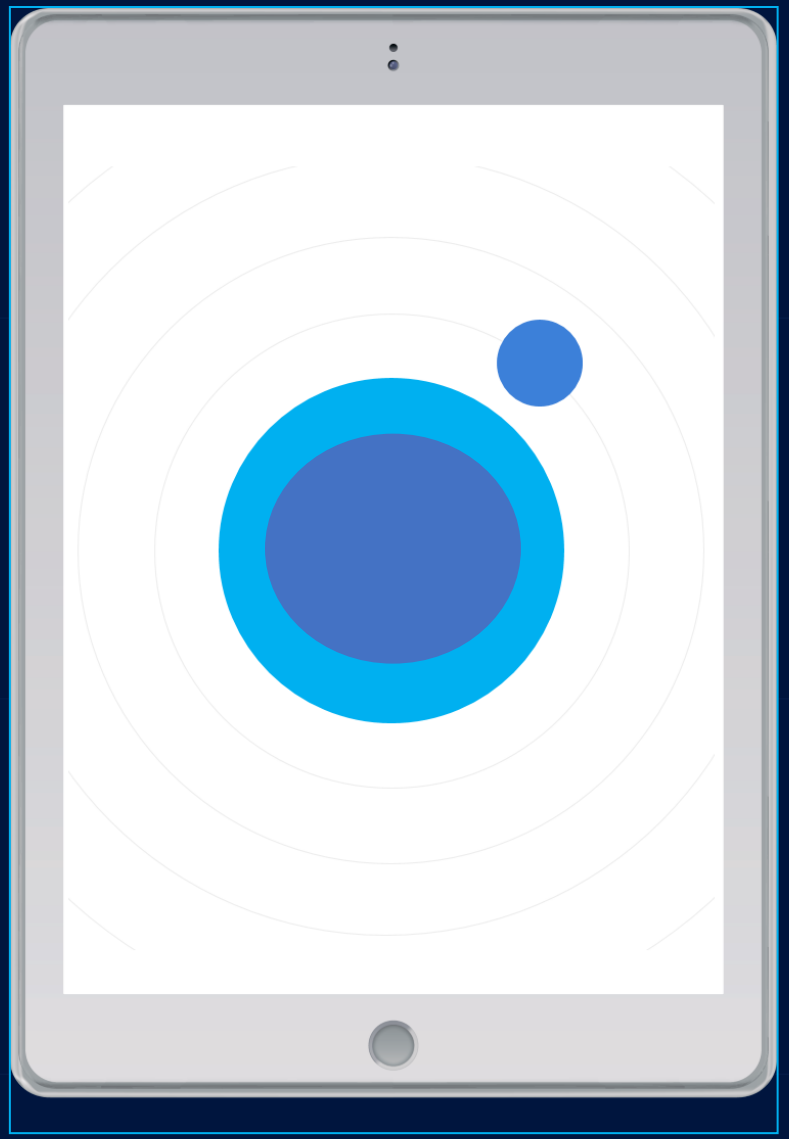
Elements of the Policy



1. Purpose
2. Scope
3. Policy Statement
4. Roles and Responsibilities
   - 4.1 Security Awareness and Training Coordinator
   - 4.2 Department Heads
   - 4.3 Employees, Contractors, and Stakeholders
5. Training Requirements
   - 5.1 Initial Training
   - 5.2 Ongoing Training
   - 5.3 Specialized Training

Elements of the Policy

6. **Security Awareness Initiatives**
   - 6.1 Awareness Campaigns
   - 6.2 Security Drills and Exercises
   - 6.3 Access to Resources
7. **Compliance and Enforcement**
   - 7.1 Monitoring and Reporting
   - 7.2 Non-Compliance
8. **Continuous Improvement**
   - 8.1 Program Evaluation
   - 8.2 Adaptation to New Threats
9. **Policy Review and Updates**



Control Impact

Direct Requirements		Indirect Requirements	
3.2.1	3.9.2	3.1.17	3.10
3.2.2	3.13	3.3	3.11
3.2.3	3.14	3.4	3.12
3.6.1		3.7	
3.6.2		3.8	
3.6.3		3.9	

Reading the Controls

NIST SP 800-171

1

Security Awareness and Training Policy

2

The 3 Trainings

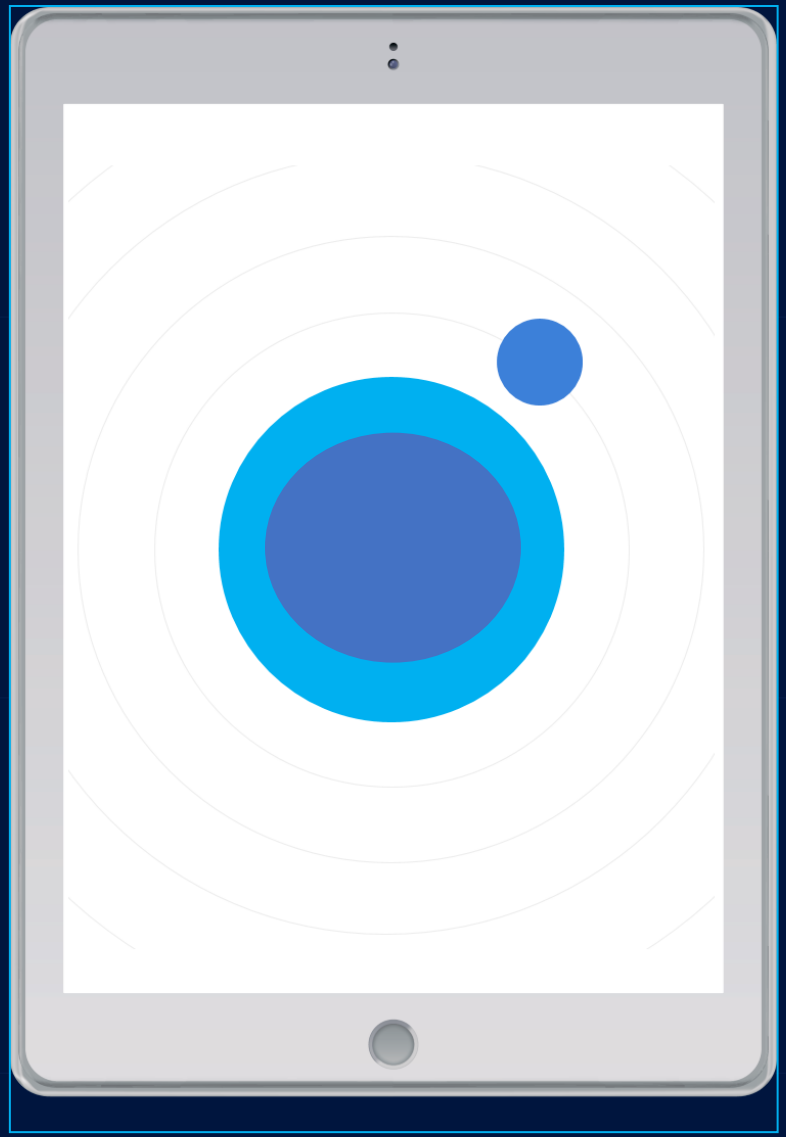
3

Maintaining a Record

3.2.1	**SECURITY REQUIREMENT** Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.2.1[a] *security risks associated with organizational activities involving CUI are identified.*
	3.2.1[b] *policies, standards, and procedures related to the security of the system are identified.*
	3.2.1[c] *managers, systems administrators, and users of the system are made aware of the security risks associated with their activities.*
	3.2.1[d] *managers, systems administrators, and users of the system are made aware of the applicable policies, standards, and procedures related to the security of the system.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Security awareness and training policy; procedures addressing security awareness training implementation; relevant codes of federal regulations; security awareness training curriculum; security awareness training materials; system security plan; training records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with responsibilities for security awareness training; personnel with information security responsibilities; personnel composing the general system user community; personnel with responsibilities for role-based awareness training]. **Test**: [*SELECT FROM:* Mechanisms managing security awareness training; mechanisms managing role-based security training].

- Understanding Cyber Threats
- Password Management
- Data Protection and Privacy
- Safe Internet and Email Practices
- Mobile Device Security
- Social Media Safety
- Physical Security
- Incident Response
- Cloud Security
- Remote Work Security
- Software and Application Security
- Risk Management and Compliance
- Personal Responsibility and Security Culture
- Security Awareness Campaigns
- Phishing Simulations and Practical Exercises

Acceptable Use Policy



Types of Bad Actors

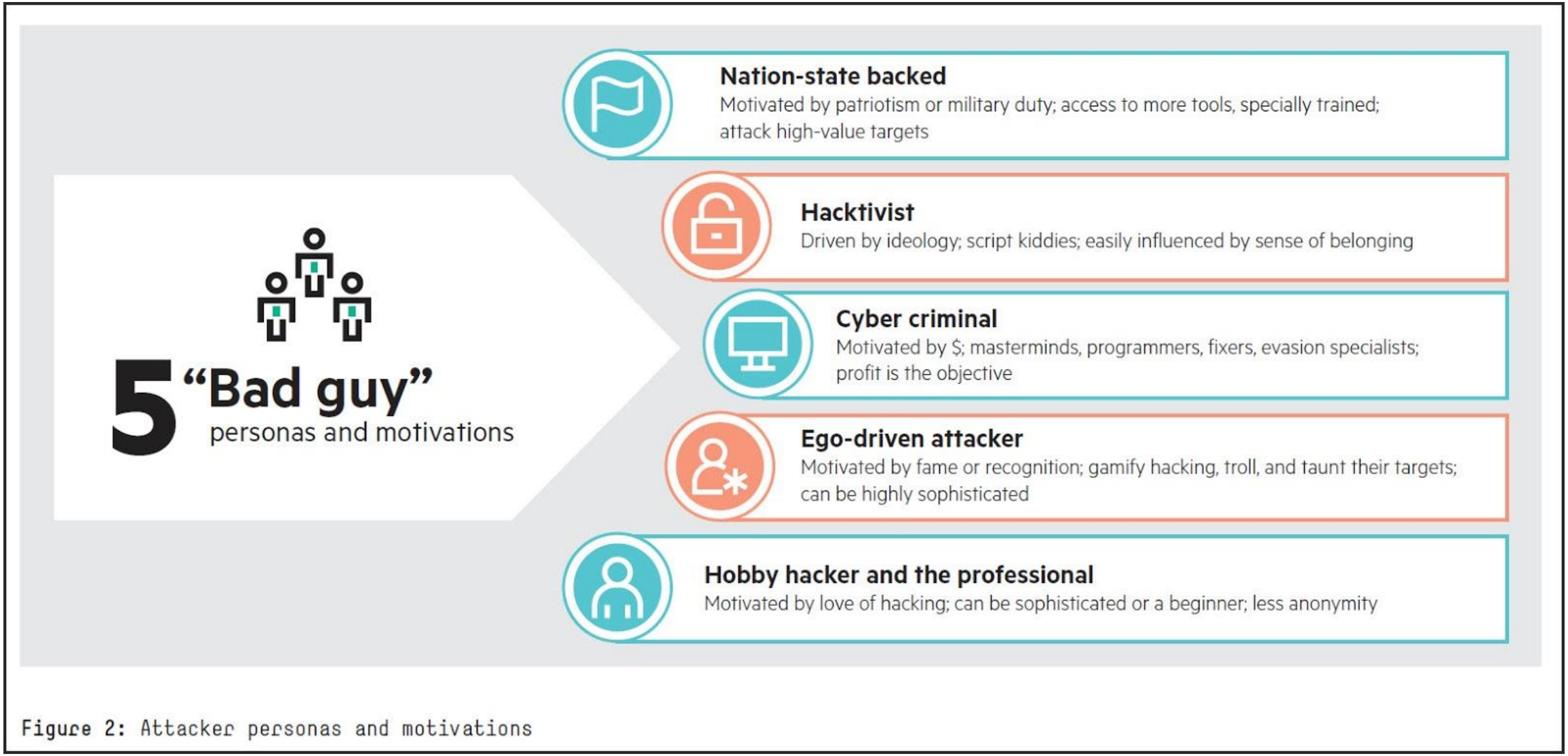
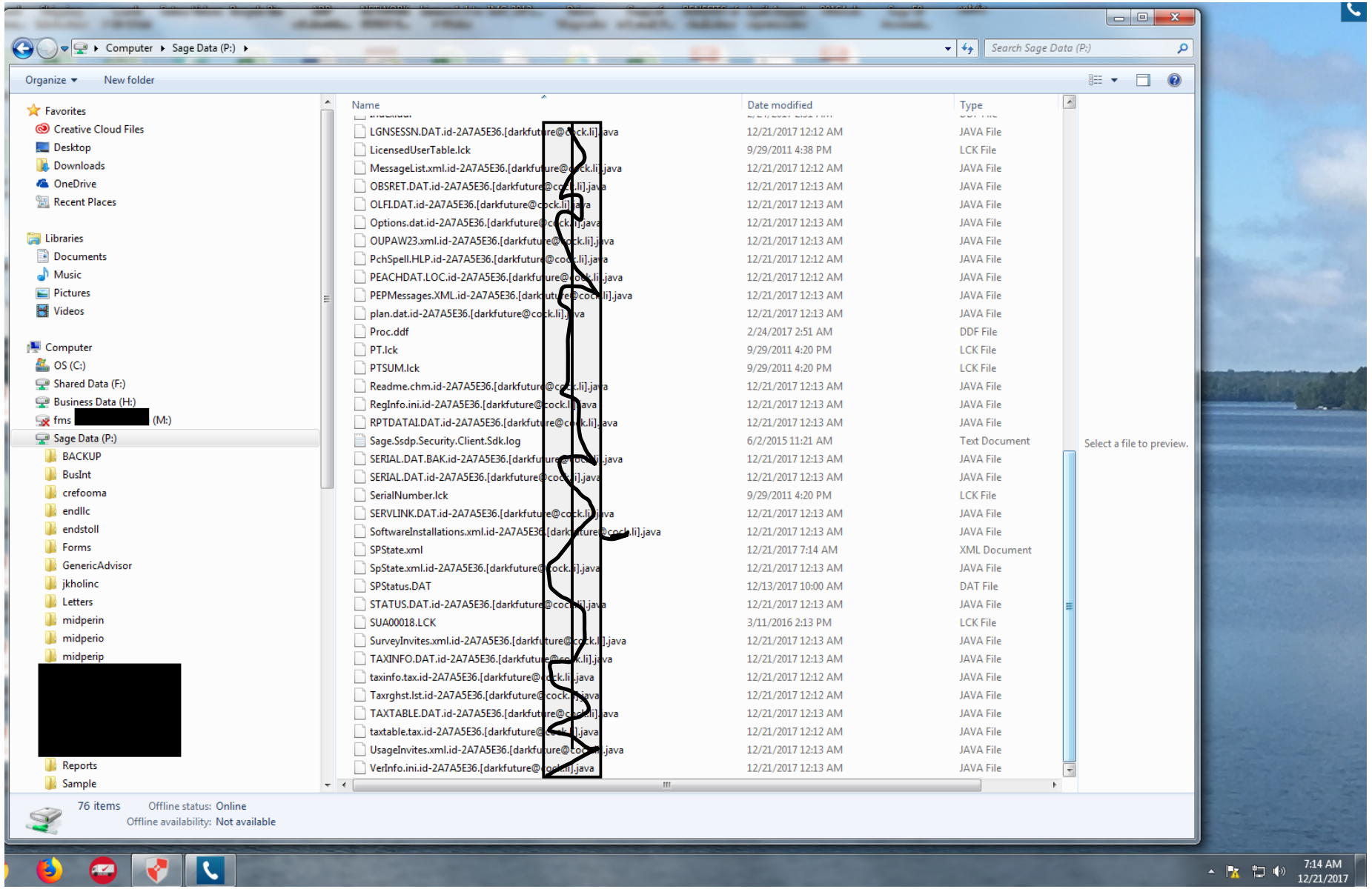
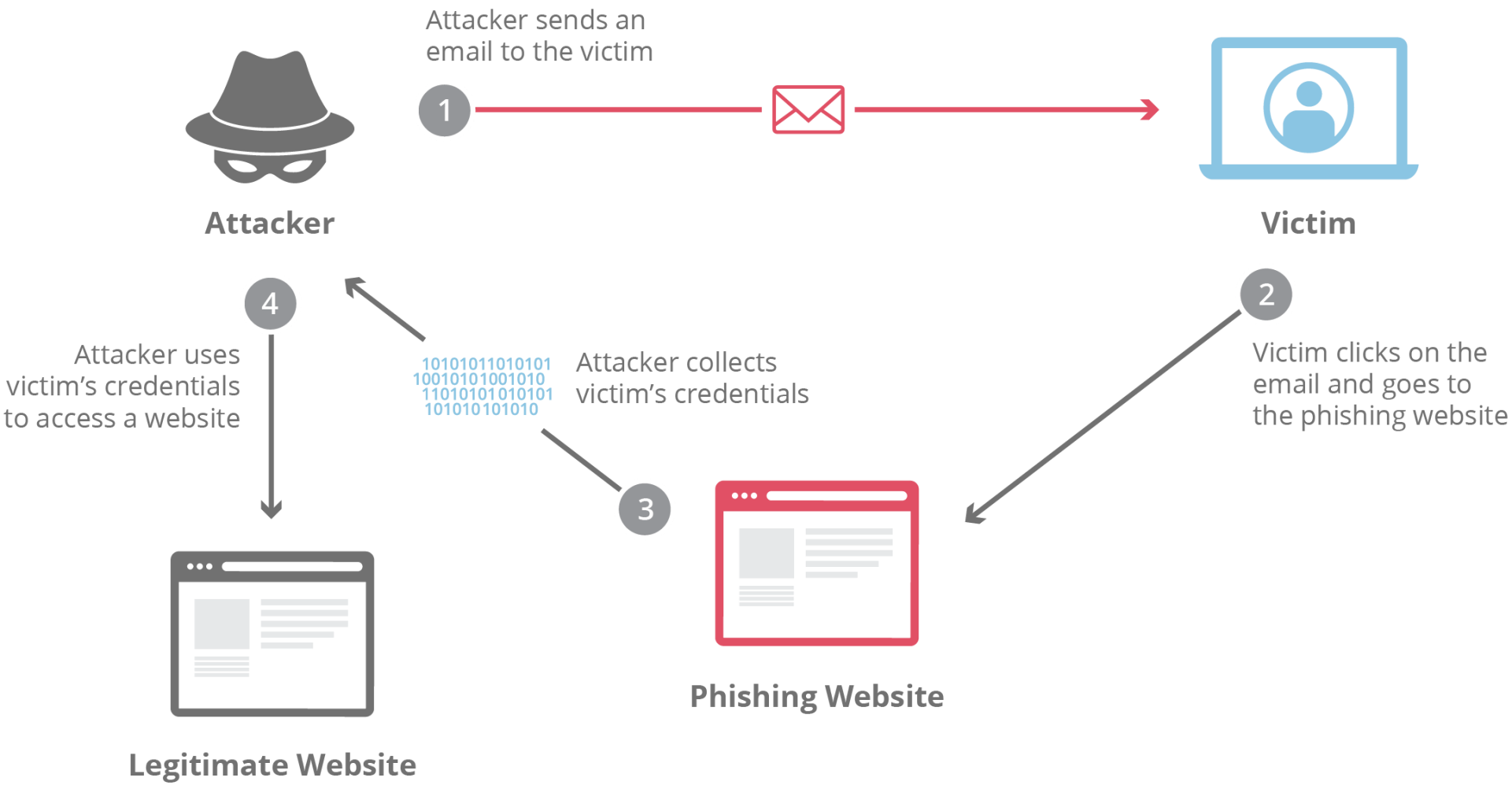


Figure 2: Attacker personas and motivations

NIST 800-171 3.3 Components



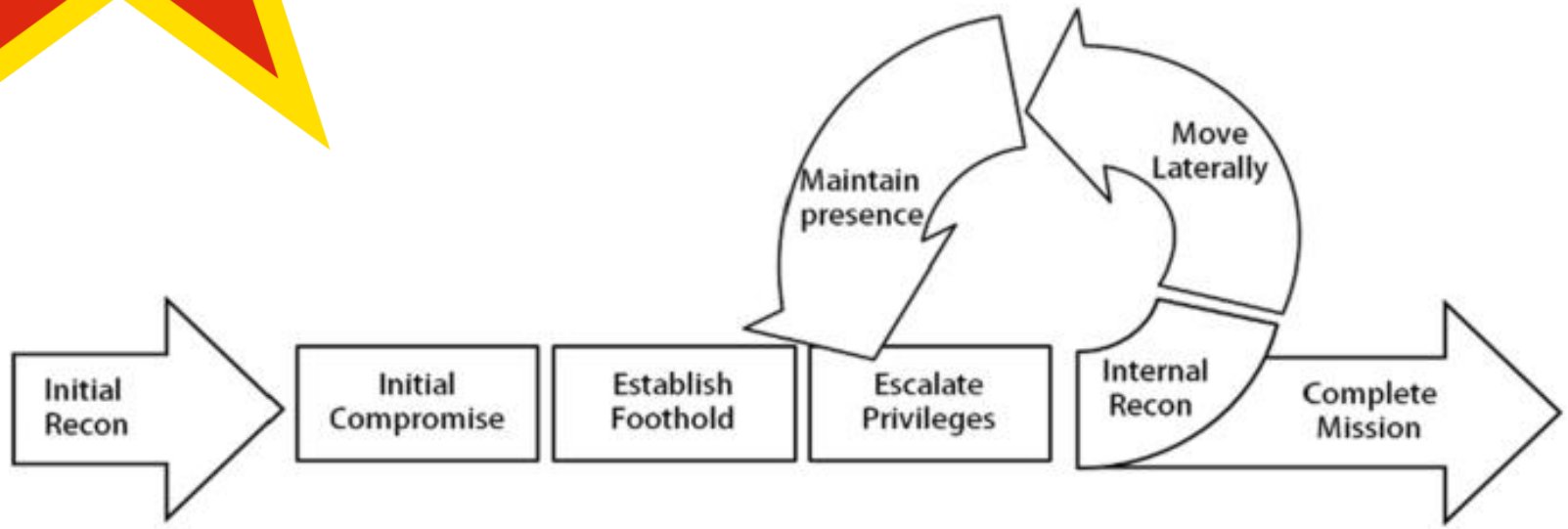
Anatomy of a Phish



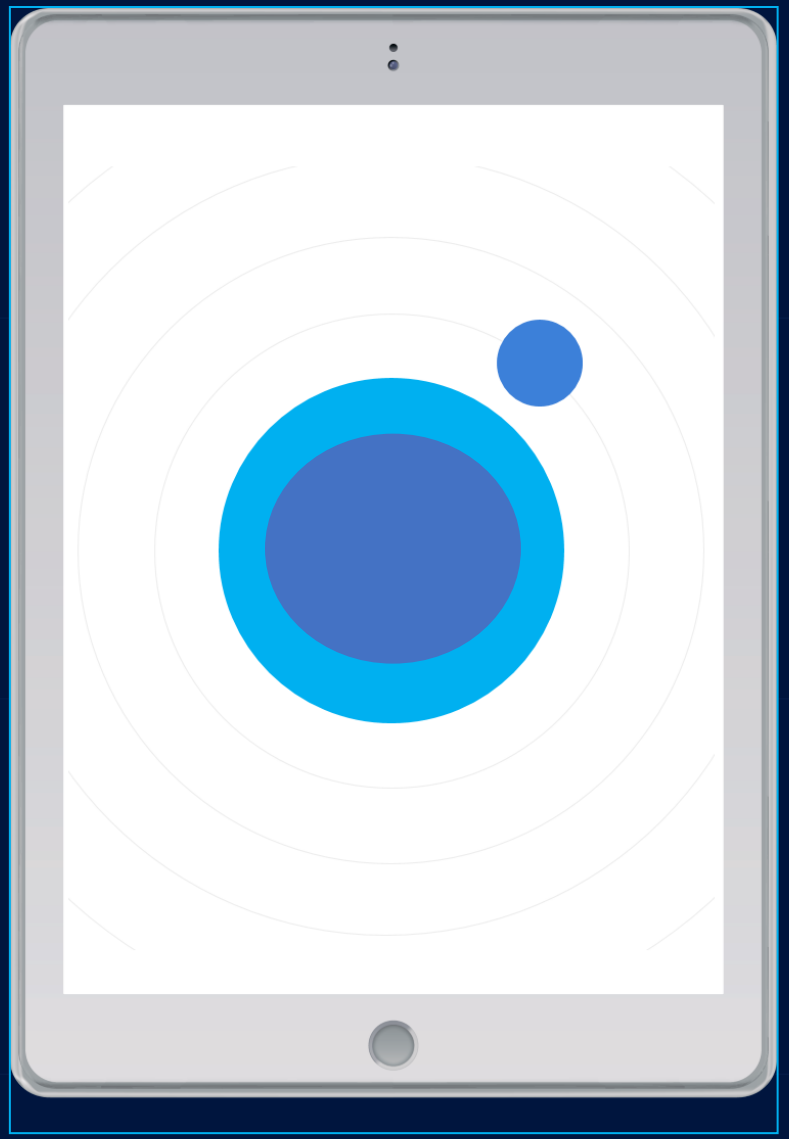
Increasingly Sophisticated

PLA Unit 61398

Pudong, Shanghai



Acceptable Use Policy



Information that is collected, created, or received pursuant to a government contract

FCI
Information that is not marked as public or for public release.
Minimum Cybersecurity Requirements in a non-federal information system:
Basic Safeguarding Clause: 48 CFR § 52.204-21*

CUI
Information that is marked or identified as requiring protection under the CUI program.
Minimum Security Requirements in a non-federal information system:
NIST SP 800-171

Public Information
Public information or information marked for public release.
Minimum Security Requirements in a non-federal information system: None

*also excludes simple transactional information.

Role-Based Trainings

3.2.2	**SECURITY REQUIREMENT** Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.2.2[a] *information security-related duties, roles, and responsibilities are defined.*
	3.2.2[b] *information security-related duties, roles, and responsibilities are assigned to designated personnel.*
	3.2.2[c] *personnel are adequately trained to carry out their assigned information security-related duties, roles, and responsibilities.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Security awareness and training policy; procedures addressing security training implementation; codes of federal regulations; security training curriculum; security training materials; system security plan; training records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with responsibilities for role-based security training; personnel with assigned system security roles and responsibilities; personnel with responsibilities

Incident Response Team

Management

- ❑ Ownership and Authority
- ❑ Leadership and Delegation
- ❑ Accountability

IT Team Leader

- ❑ Technical Response
- ❑ Translating Concerns and Solutions
- ❑ Change Log and Incident Journal
- ❑ Forensic Assistance

Operations

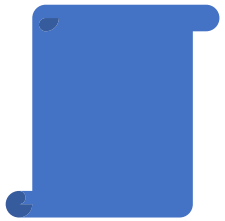
- ❑ Business Continuity
- ❑ Customer Concern Response
- ❑ Incident Intelligence

Marketing & Legal

- ❑ Customer Communications
- ❑ Reporting Requirements
- ❑ Public Statements
- ❑ Liason with Law Enforcement

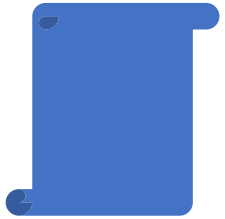
COMMUNICATIONS

Containing an Incident



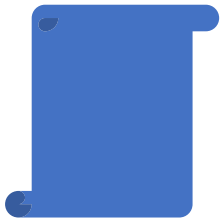
1. Isolate

- ❑ Disconnect From Network
- ❑ Do not Shutdown or Reboot
- ❑ Sandbox (Endpoint Protection)
- ❑ Approval if cannot be isolated



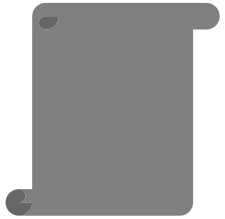
2. Indicators of Compromise

- ❑ Geographic Irregularities
- ❑ Unknown Applications
- ❑ Unusual Activity from Accounts
- ❑ Requests of Additional Permissions
- ❑ Unusual Outbound Traffic
- ❑ Increased Log-In Failures
- ❑ Database Read Volume Increases
- ❑ Unauthorized Changes



3. Copy

- ❑ Copy or Preserve Compromised Systems
- ❑ Capture Executables/Applications
- ❑ Diagram/Log/Journal Incident Details and Events

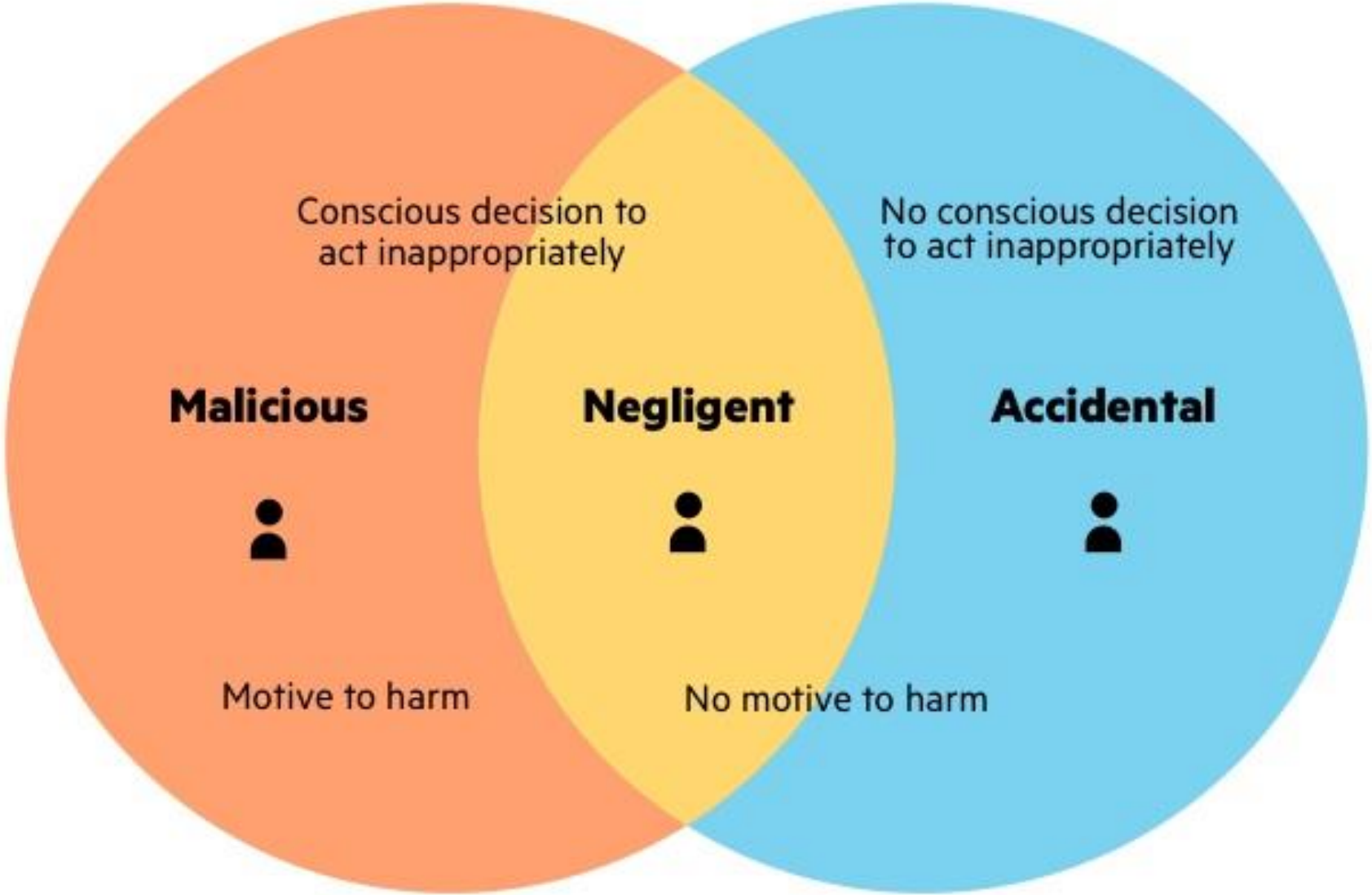


4. Backups

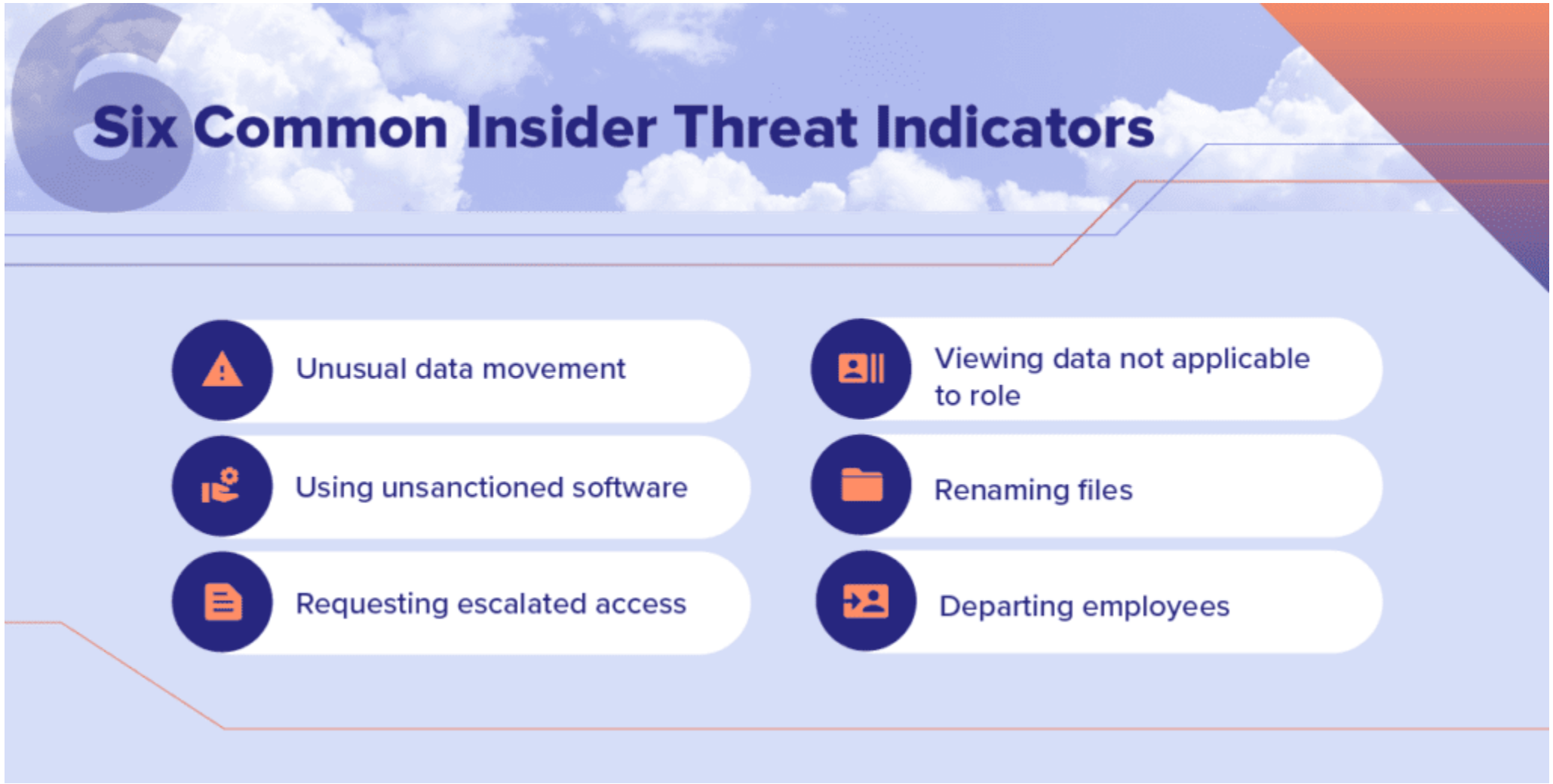
Insider Threat

3.2.3	**SECURITY REQUIREMENT** Provide security awareness training on recognizing and reporting potential indicators of insider threat.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.2.3[a] *potential indicators associated with insider threats are identified.*
	3.2.3[b] *security awareness training on recognizing and reporting potential indicators of insider threat is provided to managers and employees.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Security awareness and training policy; procedures addressing security awareness training implementation; security awareness training curriculum; security awareness training materials; insider threat policy and procedures; system security plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel that participate in security awareness training; personnel with responsibilities for basic security awareness training; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Mechanisms managing insider threat training].

Anatomy of an Insider Threat



Anatomy of an Insider Threat



Reading the Controls

NIST SP 800-171

1

Security Awareness and Training Policy

2

The 3 Trainings

3

Maintaining a Record

Pulling It All Together

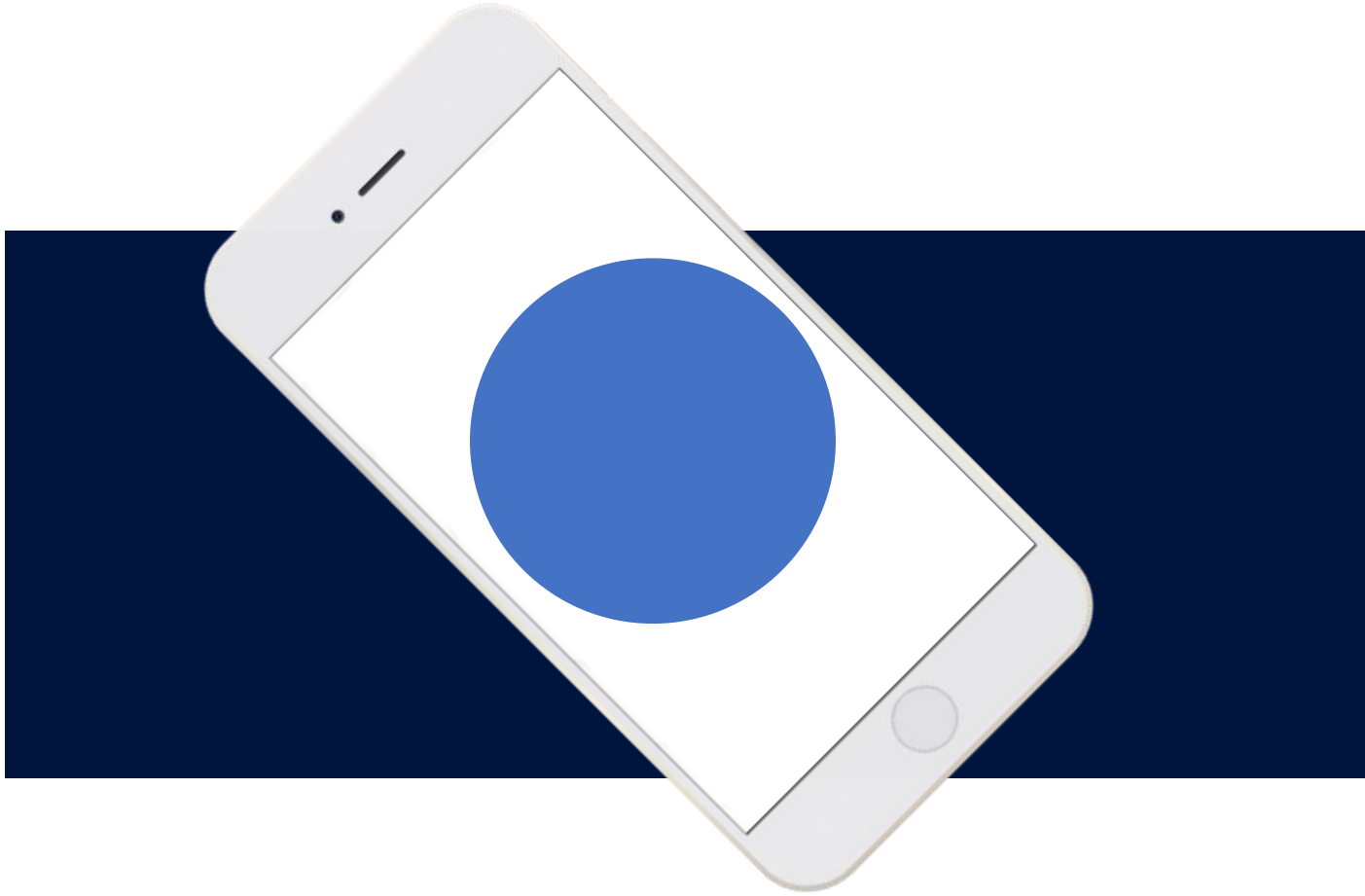
- Train Employees on Cyber Risks
- Train Those in Roles of Responsibility on proper actions
- Train employees on the nature of insider threats
- Log training efforts and completion
- Ensure Compliance

Matthew Frost

mattf@wispro.org

Wisconsin Procurement Institute

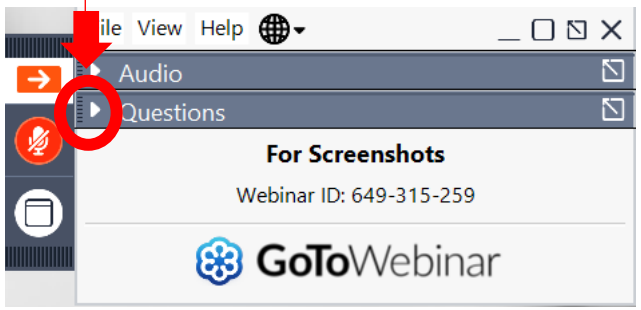
AN APEX ACCELERATOR



QUESTIONS?

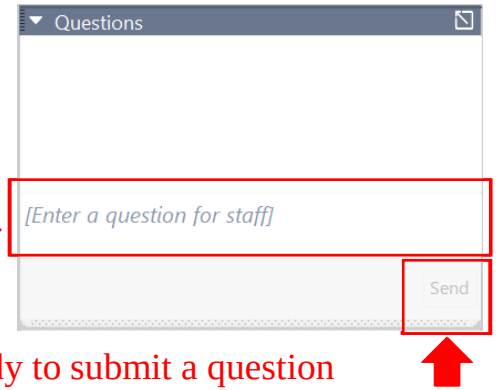
OPENING THE QUESTIONS BOX

Click here to access within the Control Panel



USING THE QUESTIONS BOX

Type questions here at any time during a presentation



Click Send when ready to submit a question

UPCOMING TRAINING - EVENTS

CYBER FRIDAY LIVE WEBINAR SERIES

Cyber Friday is a series of one-hour webinars focusing on critical topics for DOD contractors and subcontractors in cyber security, data security, and CMMC. Attendees receive 1 CPE credit for attending.

- **June 21,** 3.1.2 Security Awareness Training, Role-Based Training, and Insider Threat Training
- **July 19,** 3.1.3 Audit and Accountability Policy, Log Review Procedure
- **August 23,** 3.1.4 Configuration Management Policy, Change Request Process, Baseline Configurations
- **September 20,** 3.1.6 Incident Response Policy, Incident Response Plan
- **October 18,** 3.1.7 System Maintenance Policy
- **November 22,** 3.1.8 Media Control Policy, Media Destruction Policy and Personnel Security
- **January 24,** 3.1.11 Risk Assessment Policy, Security Assessment Reports

WPI Wisconsin Procurement Institute
An APEX Accelerator

…More information and registrations at wispro.org/events

EMERGING ISSUES WEBINAR SERIES

This series is intended as an information tool and resource for contract managers and those with a compliance function. Attendees receive 1 CPE credit for attending.

- **July 25** – Beyond contracts: Conducting Business with the Federal Government
- **Aug 22** – Regulation Making – The Process and the Important Role Businesses Play
- **Sep 19** – Industry 4.0 – The Next Generation of the DIB
- **Oct 24** – Innovation – What Does Innovation Look Like from DoD's Perspective?
- **Nov 21** – The Critical Role Your Accounting System Plays in SBIR/STTR Success

WPI Wisconsin Procurement Institute
An APEX Accelerator

…More information and registrations at wispro.org/events

18th Annual Wisconsin Government Opportunities Business Conference (GOBC)

In Partnership with Wisconsin's Military Installations

July 10

Truax Field

GOBC will provide you the opportunity to gain insights into:

- *COFFEE with the COMMANDER*
- Current operations and priorities at Wisconsin's Federal and State government agencies and military facilities
- Connecting with agency and installation leadership, operational staff and buyers
- Locating and bidding on current and future procurement opportunities
- Resources available to assist your business in winning government prime and subcontracts

…More information and registrations at wispro.org/events

WPI Wisconsin Procurement Institute
An APEX Accelerator

NCMA National Contract Management Association
WISCONSIN

- Save the Date -

The Contracting Academy

Developing and Growing Government Contractors

Dec 10

Virtual | 9:00 am - 4:00 pm

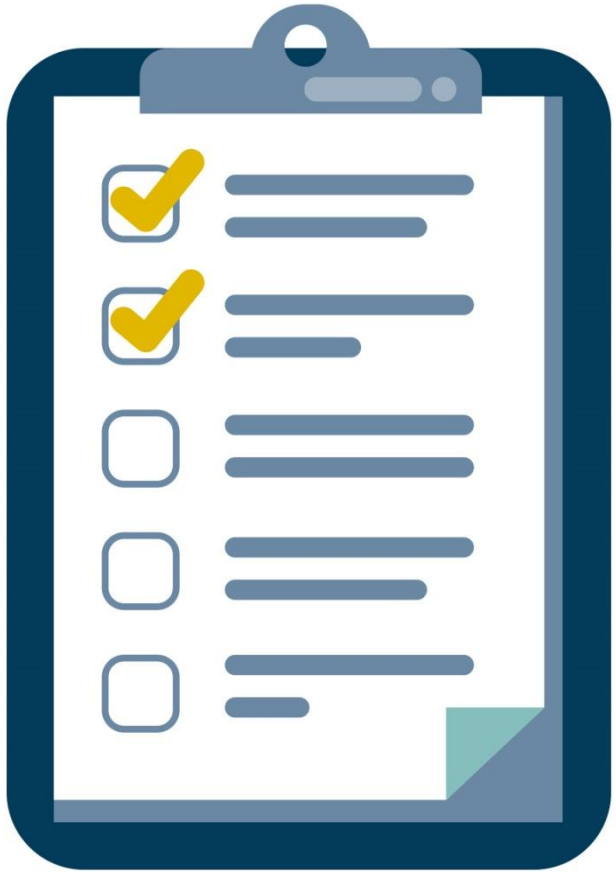
The Contracting Academy (TCA) is an opportunity for businesses to grow their technical knowledge of contracting with Federal Government, State/Local Government, and Government Prime Contractors. The series of workshops will benefit established businesses looking to grow and develop their government sales.

…More information and registrations at wispro.org/events

WPI Wisconsin Procurement Institute
An APEX Accelerator

NCMA National Contract Management Association
WISCONSIN

SURVEY



Wisconsin Procurement Institute
An APEX Accelerator

June 21, 2024

NCMA
NATIONAL CONTRACT MANAGEMENT ASSOCIATION
WISCONSIN

CONTINUING PROFESSIONAL EDUCATION

This webinar is eligible for 1 CPE credit.
For a certificate of this credit please contact:

Neelu Patil
neelagangap@wispro.org

PRESENTED BY

Wisconsin Procurement Institute (WPI)

www.wispro.org

Matt Frost

Wisconsin Procurement Institute

MattF@wispro.org | 608-293-0920

10437 Innovation Drive Suite 320
Milwaukee WI 53226