Wisconsin Procurement Institute

AN APEX ACCELERATOR

APEX ACCELERATORS

CYBER FRIDAY:

The Forensic Record

April 14, 2023 @ 11:00 am - Noon

Presented by Matt Frost, WPI

Wisconsin Procurement Institute

AN APEX ACCELERATOR

Cyber Friday

Webinar Etiquette

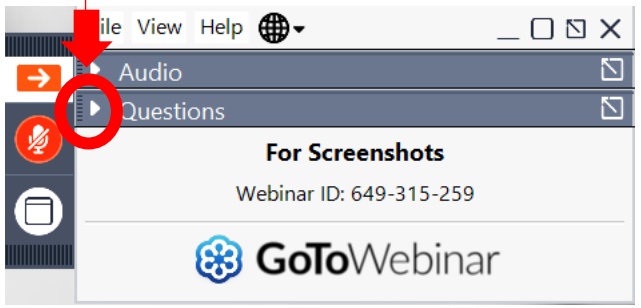
PLEASE

- 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!

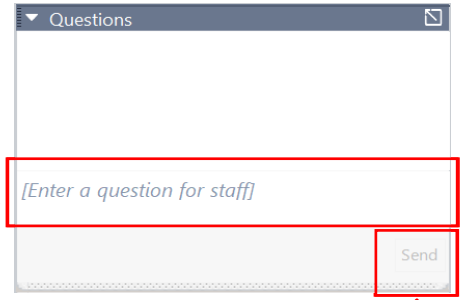
OPENING THE QUESTIONS BOX

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

WPI is Wisconsin's APEX ACCELERATOR

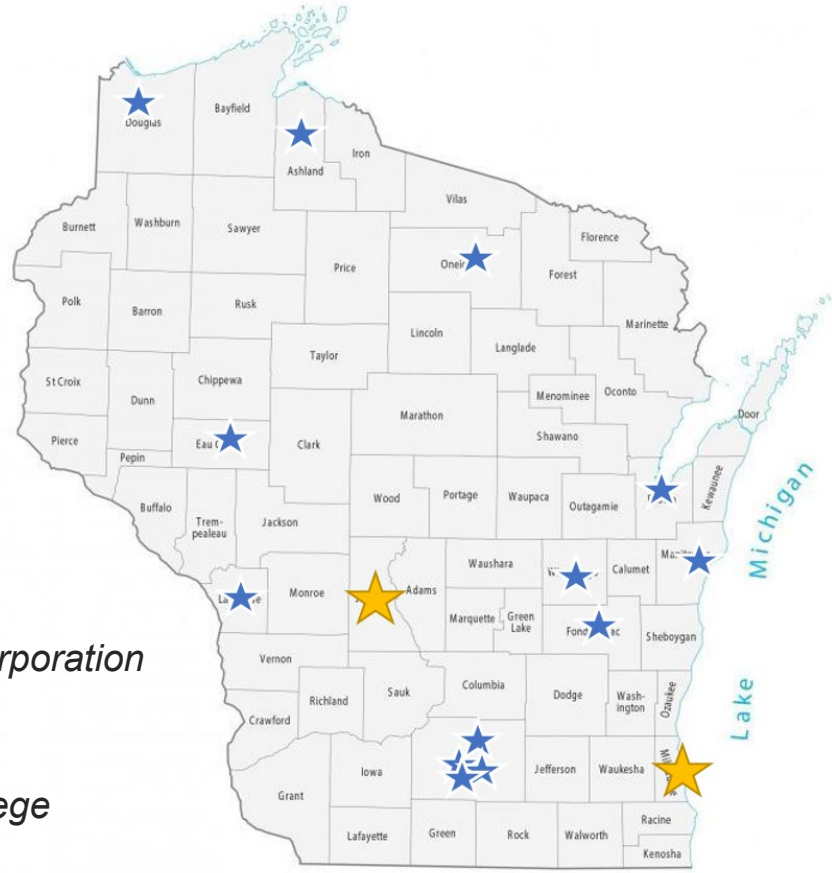
The APEX Accelerators program, under management of the Department of Defense (DOD) Office of Small Business Programs (OSBP), plays a critical role in the Department's efforts to identify and engage with a wide range of businesses entering and participating in the defense supply-chain. The program provides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

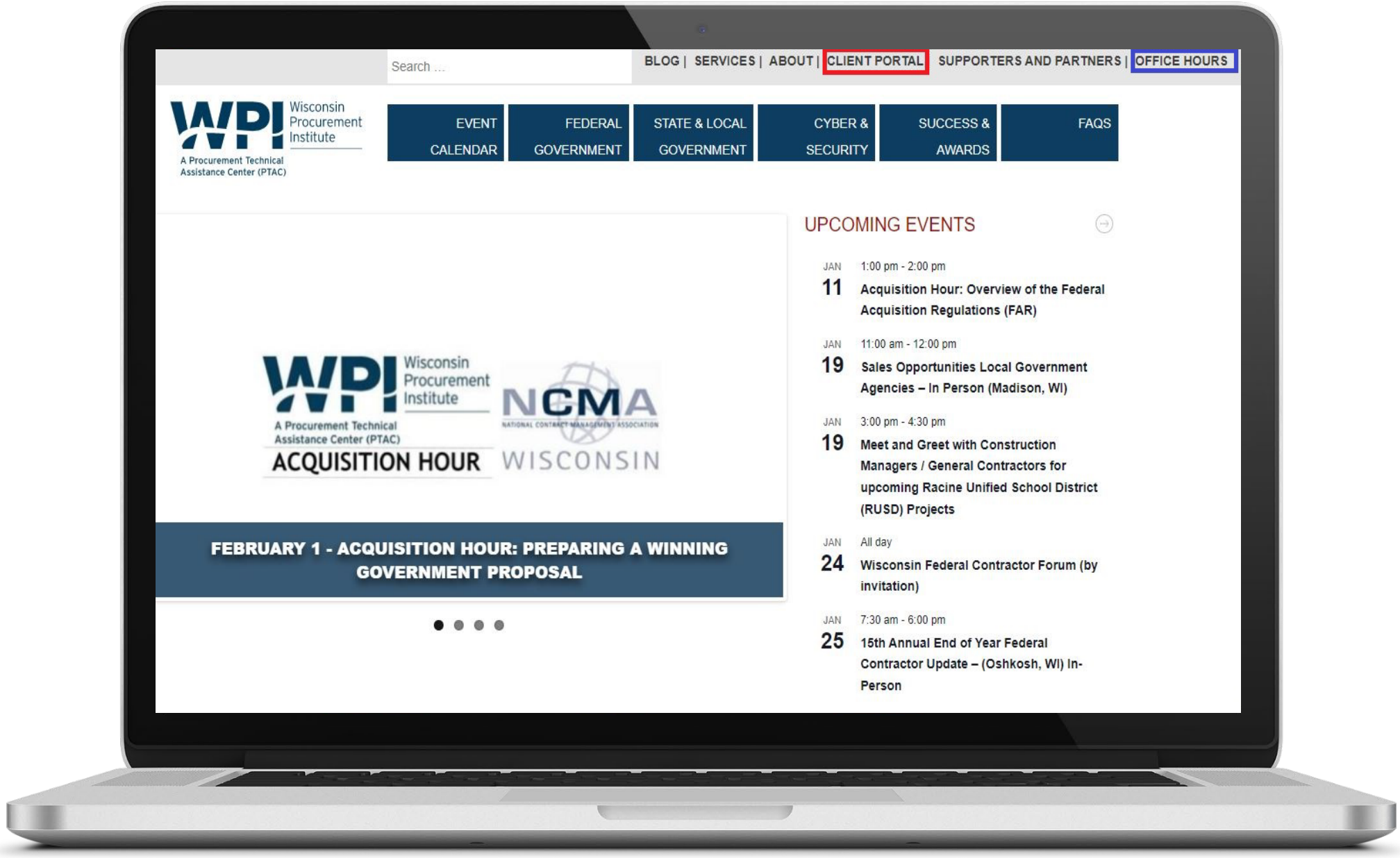
More about WPI

- 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……
- Last year WPI sponsored or participated in over 80 events
- Last year WPI provided technical assistance to over 1300 companies
- The APEX Accelerator is funded in part through a cooperative agreement with the Department of Defense
- WPI is also funded by the Wisconsin Economic Development Corporation (WEDC), contributions and in-kind

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)*
- **ASHLAND**
  - *Ashland Area Development Corporation*
- **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*
- **RHINELANDER**
  - *Nicolet Area Technical College*
- **SUPERIOR**
  - *Small Business Dev Center; UW Superior*

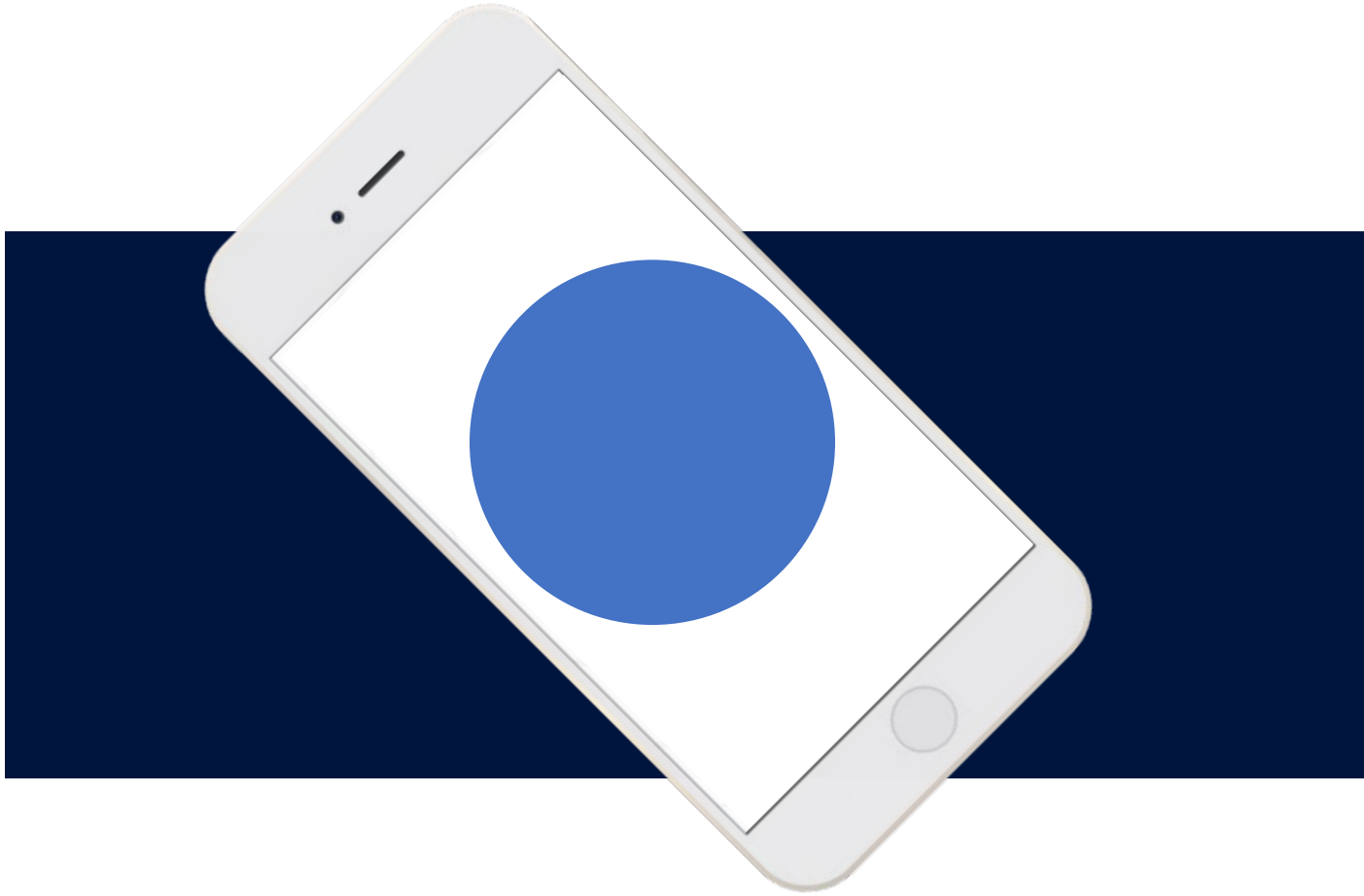



Search ...
BLOG | SERVICES | ABOUT | CLIENT PORTAL SUPPORTERS AND PARTNERS | OFFICE HOURS
Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
EVENT CALENDAR
FEDERAL GOVERNMENT
STATE & LOCAL GOVERNMENT
CYBER & SECURITY
SUCCESS & AWARDS
FAQS
Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
ACQUISITION HOUR
NCMA
WISCONSIN
FEBRUARY 1 - ACQUISITION HOUR: PREPARING A WINNING GOVERNMENT PROPOSAL
UPCOMING EVENTS
JAN 11 1:00 pm - 2:00 pm Acquisition Hour: Overview of the Federal Acquisition Regulations (FAR)
JAN 19 11:00 am - 12:00 pm Sales Opportunities Local Government Agencies – In Person (Madison, WI)
JAN 19 3:00 pm - 4:30 pm Meet and Greet with Construction Managers / General Contractors for upcoming Racine Unified School District (RUSD) Projects
JAN 24 All day Wisconsin Federal Contractor Forum (by invitation)
JAN 25 7:30 am - 6:00 pm 15th Annual End of Year Federal Contractor Update – (Oshkosh, WI) In-Person

The Forensic Record

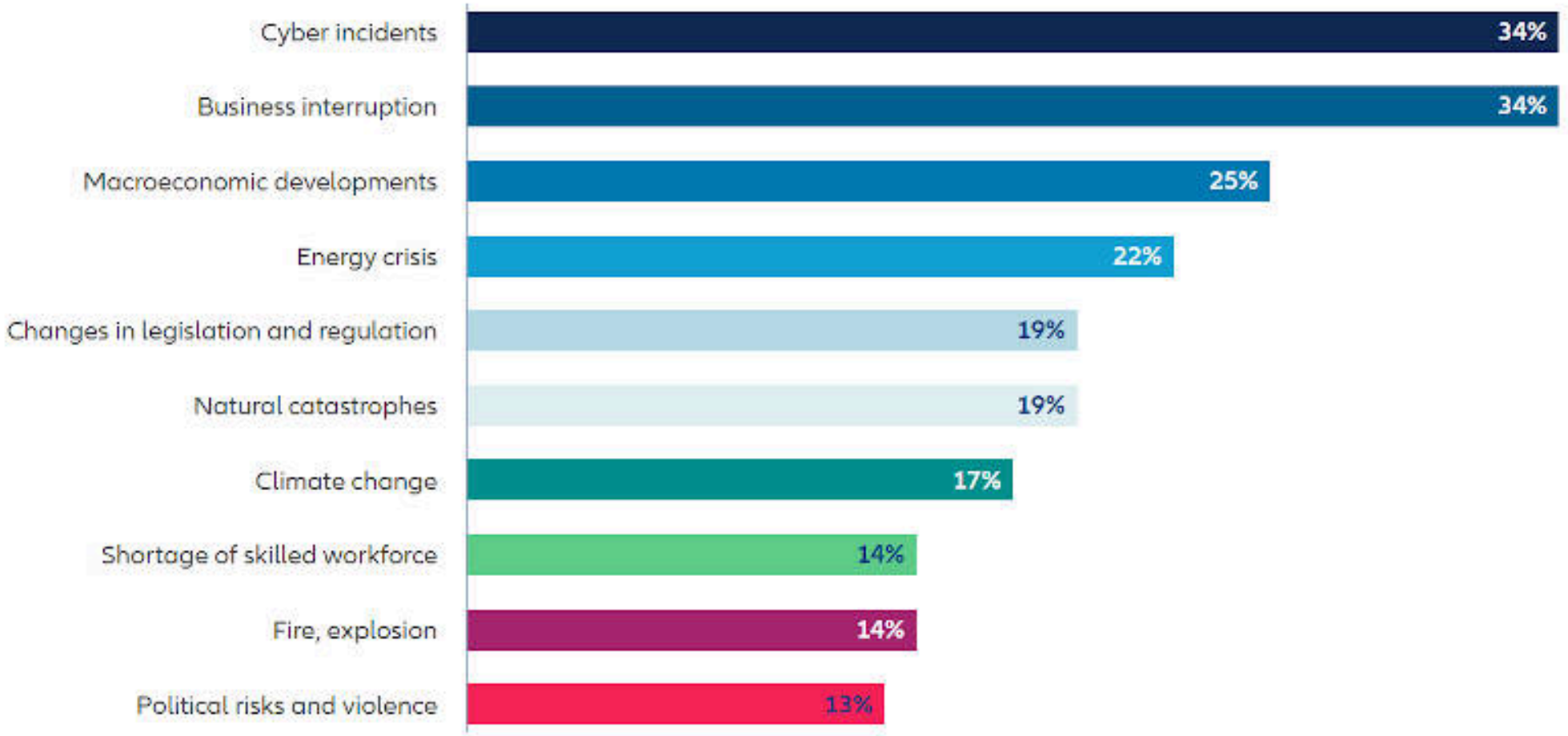
Wisconsin Procurement Institute

AN APEX ACCELERATOR



CYBER FRIDAY SESSIONS – April 14th, 2023

Why prepare?



Source: Allianz Risk Barometer 2023

The numbers represent the percentage of all participants who responded (2,712). The numbers do not add up to 100% because more than one risk could be selected.

DFARS 252.204-7012

NIST
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.

3.3.1
Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

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.

1. NIST SP 800-61
   NIST Special Publication 800-92
   Guide to Computer Security Log Management
2. CISA
   Department of Homeland Security's Cybersecurity & Infrastructure Security Agency
3. NIST SP 800-171 R2
   NIST Special Publication 800-171 R2
   Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

The Incident Response Plan

NIST SP 800-61

1 — INTENT

2 — LOGS & RECORDS

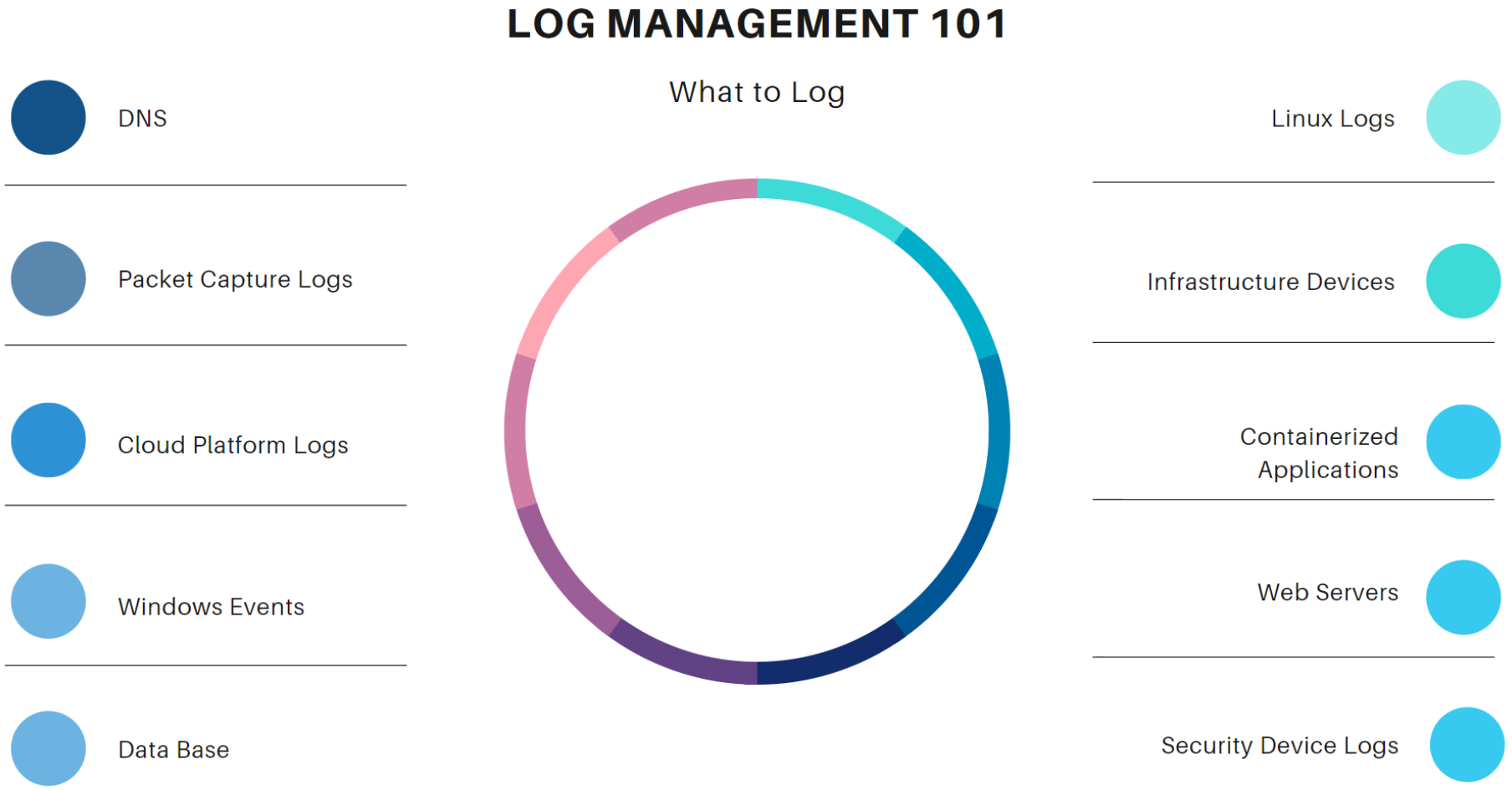
3 — CONSIDERATIONS

Incident Response

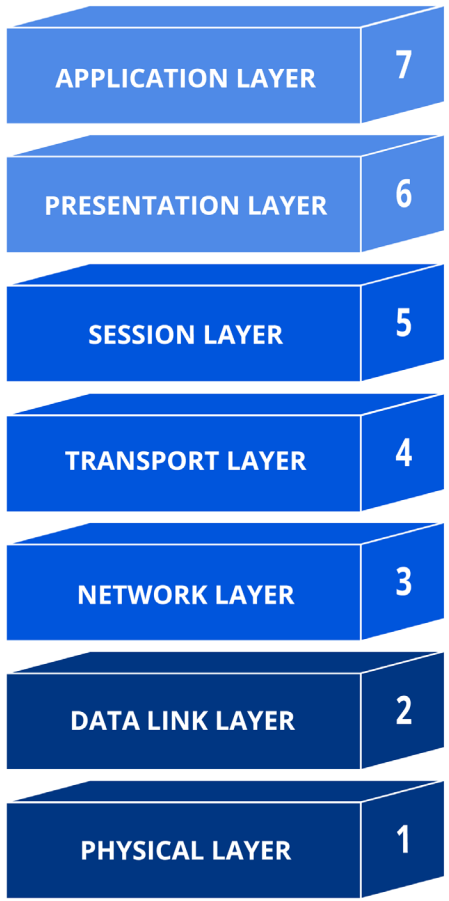
Audit and Accountability

- Create Logs
- Identify Users/Services
- Review and Update Events
- Alerting
- Review, Analyze, and Report
- Record Reduction and Reporting
- Preserve the Timeline
- Secure and Protect

What to Log?


LOG MANAGEMENT 101
What to Log
DNS
Packet Capture Logs
Cloud Platform Logs
Windows Events
Data Base
Linux Logs
Infrastructure Devices
Containerized Applications
Web Servers
Security Device Logs

The OSI Model – Open Systems Interconnection



— Human-computer interaction layer, where applications can access the network services

— Ensures that data is in a usable format and is where data encryption occurs

— Maintains connections and is responsible for controlling ports and sessions

— Transmits data using transmission protocols including TCP and UDP

— Decides which physical path the data will take

— Defines the format of data on the network

— Transmits raw bit stream over the physical medium

Roles and Responsibilities

01

Security Administrator

Responsible for the configuration, capture, analysis, and maintenance of the logs.

02

Incident Response Team

Responsible for the review, risk management, and decision making when presented with log analysis.

03

Audit & Review

Responsible for ensuring log data is preserved, accurate, and capable of being correlated and analyzed.

04

Process & Planning

Determines log management intentions, operations, and procedures.

The Incident Response Plan

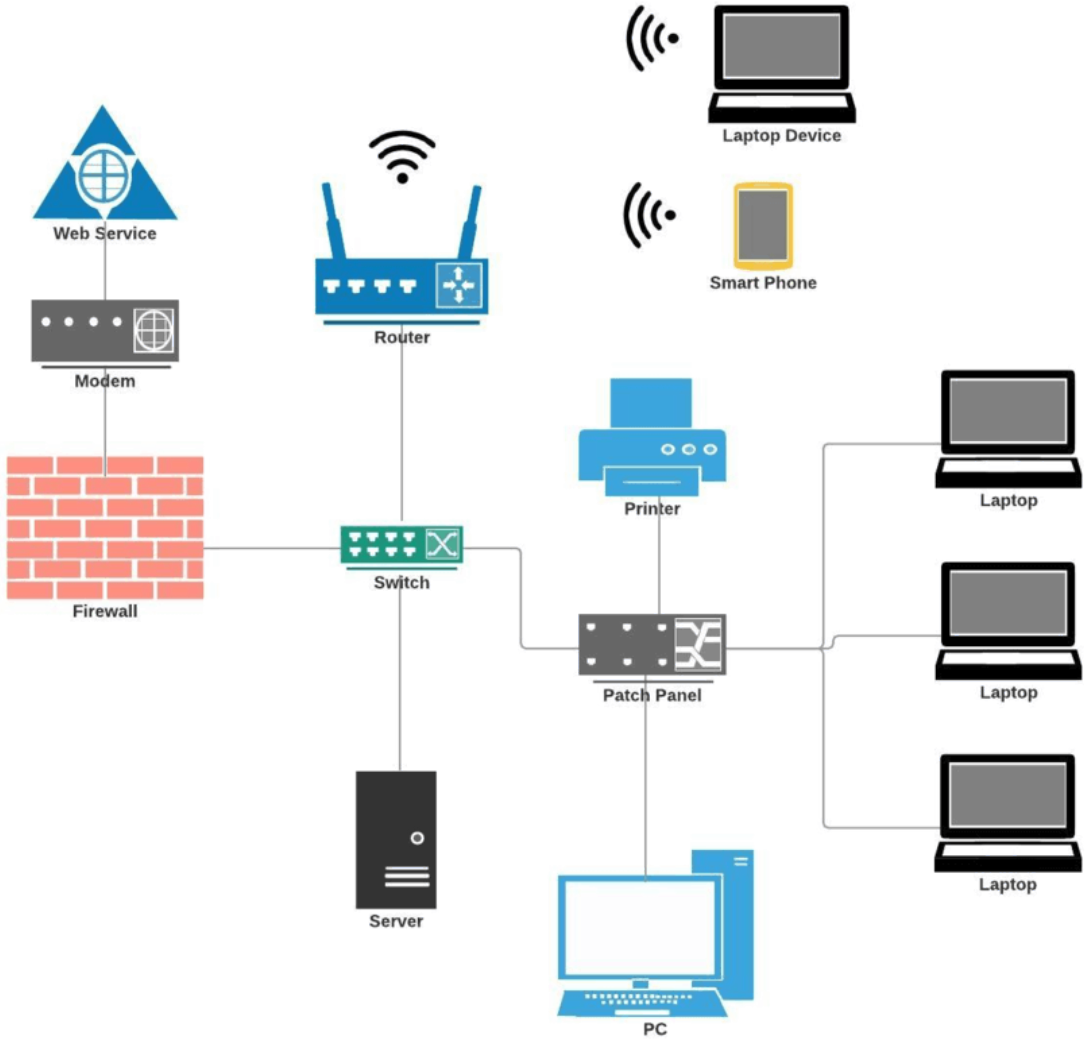
NIST SP 800-61

1 — INTENT

2 — LOGS & RECORDS

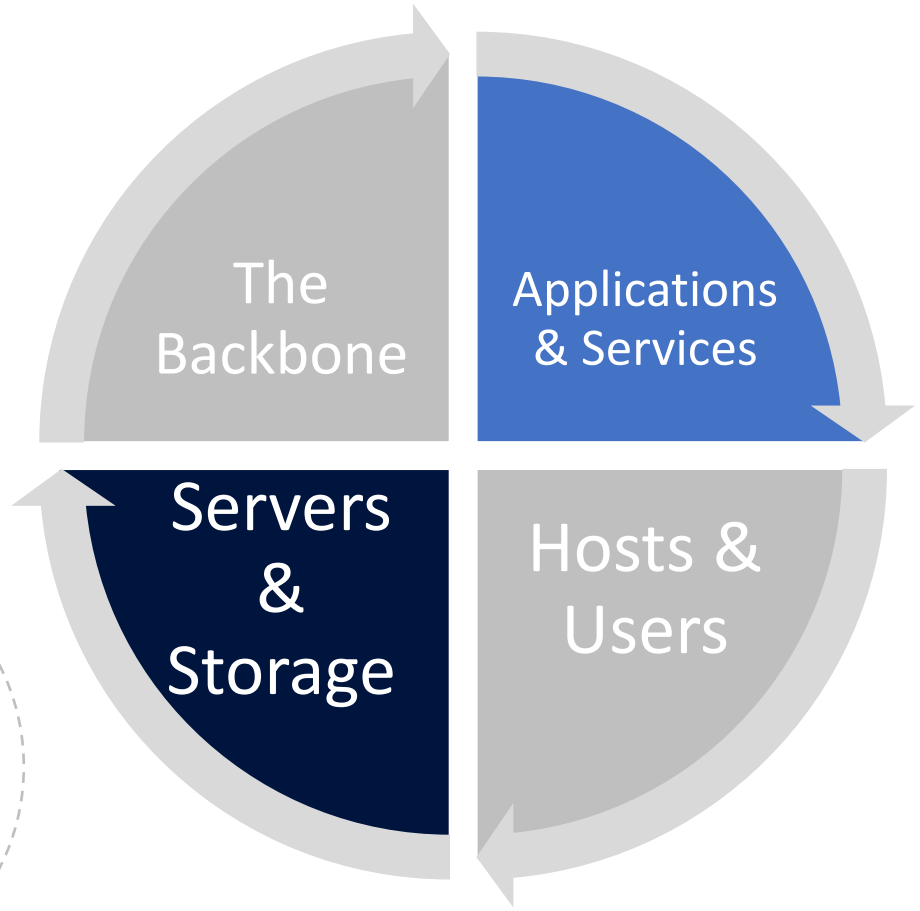
3 — CONSIDERATIONS

The Battlefield



The Correlative Process

Capturing a comprehensive picture of your data usage is critical to discover, identify, and mitigate incidents.



Practical limitations for SMBs can make log collection/analysis difficult – focus on a solid start and expand as resources allow and necessity demands.

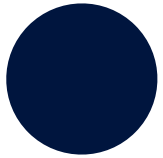
61%

Of SMBs Were Targeted in 2021

11%

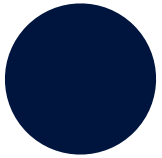
Of SMBs Logged Appropriately

What to capture?



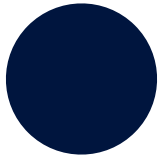
REQUESTS

Record each request or invocation of service within the application. Ex: Services, API Access, Process Start Up, Application Access



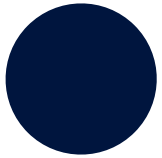
AUDIT TRAIL

Any change to data including creating, updated, deleting, or exporting data. Includes identity, date and time, and what data was involved.



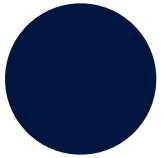
AVAILABILITY

Faults and exceptions that impact availability and stability of system components. Ex: Capacity Limit, Usage, Errors or Bugs, Connectivity, Latency/Response



THREATS

Suspicious activities and events. Ex: Unauthorized access to processes or data, invalid parameters or input, failed authentication attempts, failed verifications, warnings/alerts.



EVENTS

Any activity that a user can make on/in an application or system. Ex: Search Queries, File Views, Shares, Time Spent on Data, Behavioral Histories

SECURING THE RECORD

CONTROL ACCESS

Designated administrators (not all administrators, necessarily). Principle of Least Privilege.

STORE AND ENCRYPT

Log files should be stored for a period of no-less than 90 Days and encrypted to preserve their integrity.

BACKUP

Log files should be backed up regularly and preserved in multiple locations.

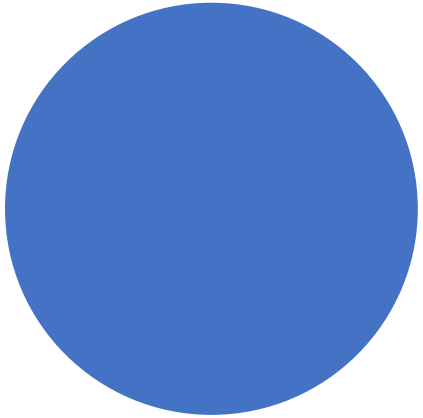
1 INTENT

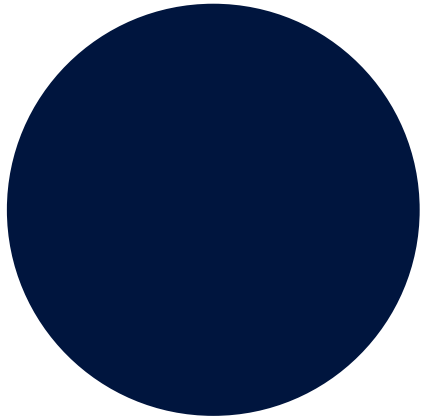
2 LOGS & RECORDS

3 CONSIDERATIONS

ADDITIONAL DOCUMENTATION

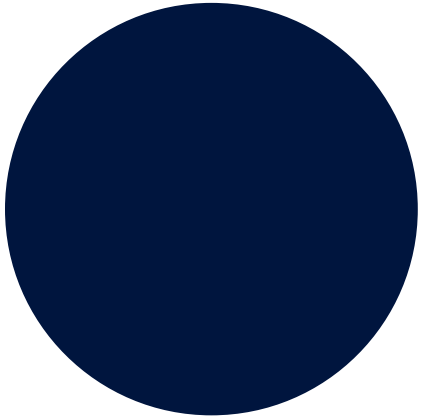
Timeline/Journal of Incidents

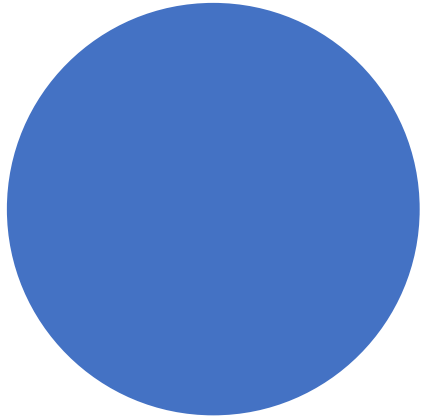




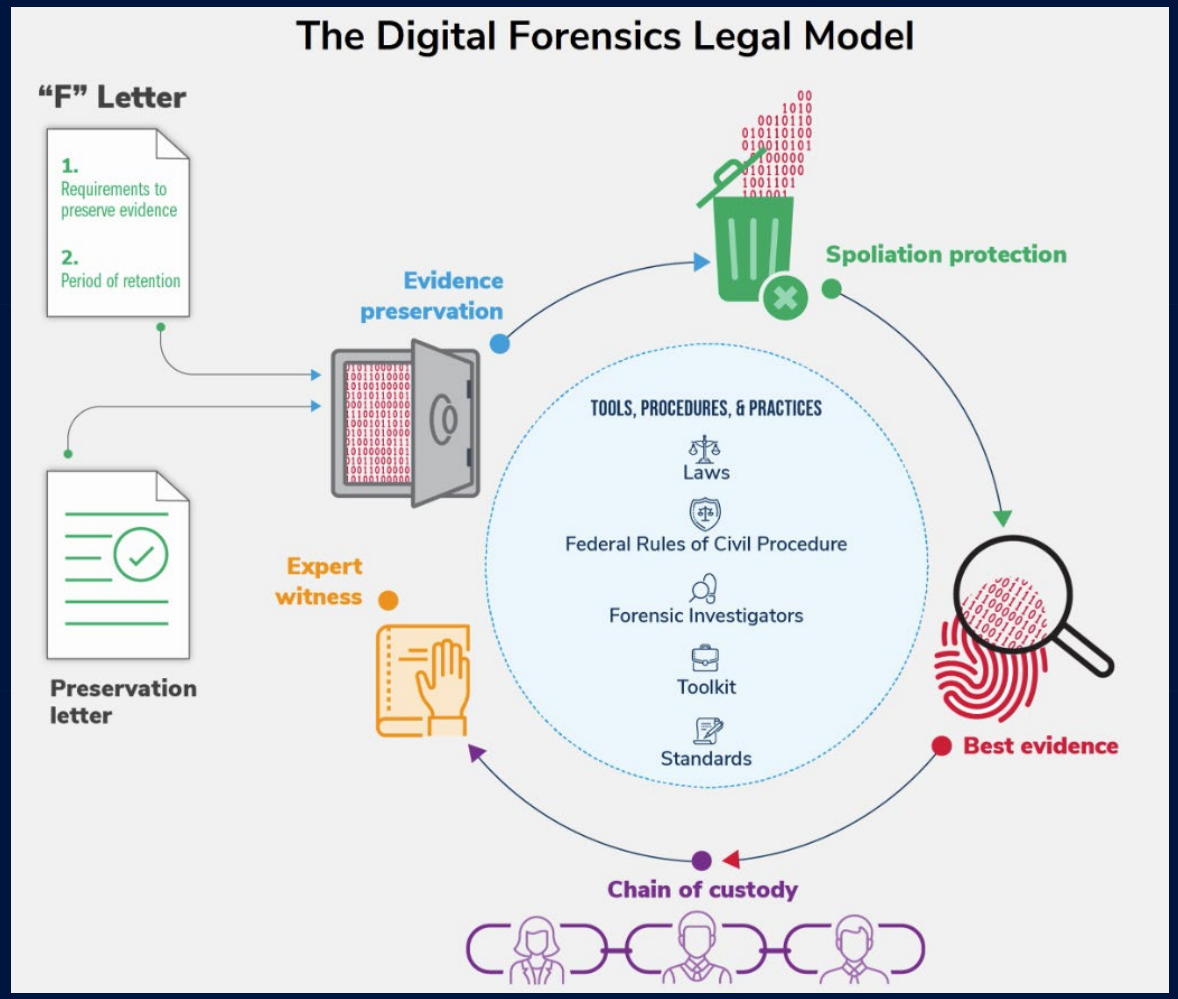
Incident Response Team's communications/meeting minutes.

Person of Authority





Chain of Custody



THINGS TO DO

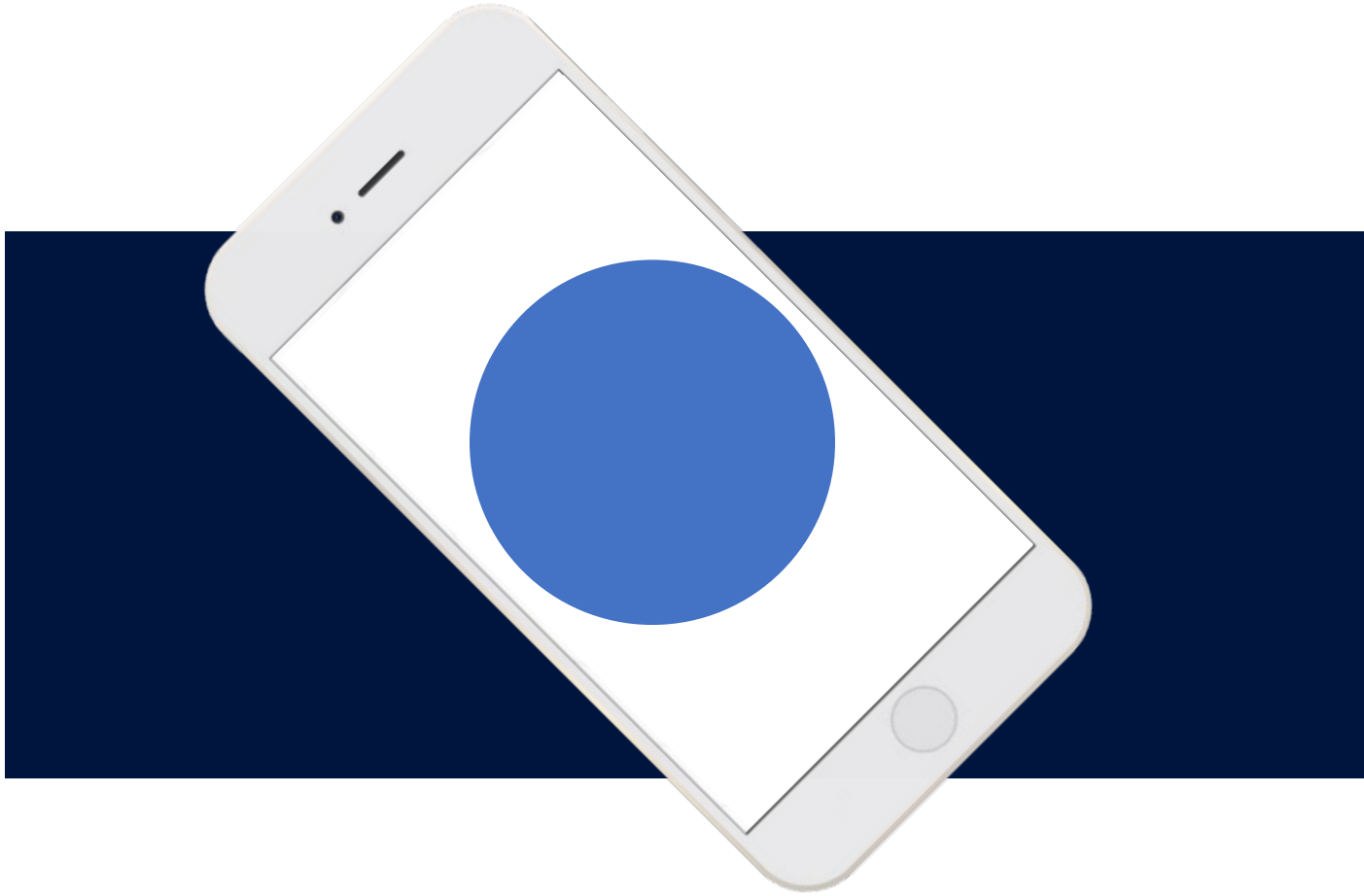
- ✓ Preserve Power State (No Shutdowns or Startups)
- ✓ Create Copy or Image
- ✓ Establish Physical Custody
- ✓ Document Chain of Custody
- ✓ Be Familiar with Laws and Process

Matthew Frost

mattf@wispro.org

Wisconsin Procurement Institute

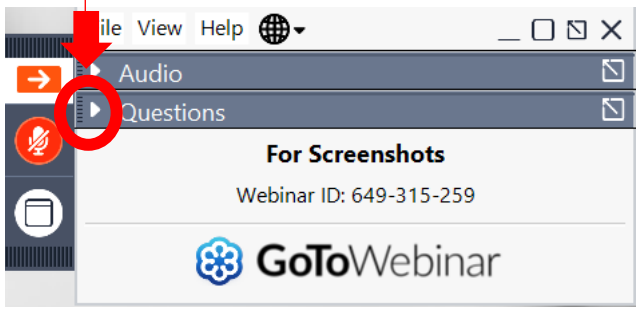
AN APEX ACCELERATOR



QUESTIONS?

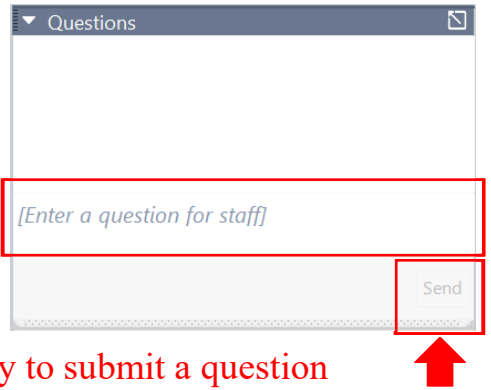
OPENING THE QUESTIONS BOX

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

- ~~March 24~~
  ~~Protecting the Data~~

- April 14
  The Forensic Record

- April 28
  Culture of Security

PRESENTED BY

WPI Wisconsin Procurement Institute
AN APEX ACCELERATOR
Cyber Friday

TECHNOLOGY INNOVATION CENTER at Research Park

NCMA National Contract Management Association WISCONSIN

APEX ACCELERATORS

The Contracting Academy

Developing and Growing Government Contractors

Presents:

9th Annual DOD Contract Management Update

–VIRTUAL–

May 2-3, 2023

Visit WIContractingAcademy.org

WPI Wisconsin Procurement Institute
A DOD APEX ACCELERATOR

NDIA Great Lakes

NCMA National Contract Management Association WISCONSIN

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

April 14, 2023

SURVEY

Wisconsin Procurement Institute
AN APEX ACCELERATOR

April 14, 2023

APEX ACCELERATORS

CONTINUING PROFESSIONAL EDUCATION

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

Caroline Boettcher
carolineb@wispro.org

PRESENTED BY

Wisconsin Procurement Institute (WPI)
www.wispro.org

Matthew Frost
Wisconsin Procurement Institute
mattf@wispro.org | 608.293.0920

10437 Innovation Drive Suite 320
Milwaukee WI 53226