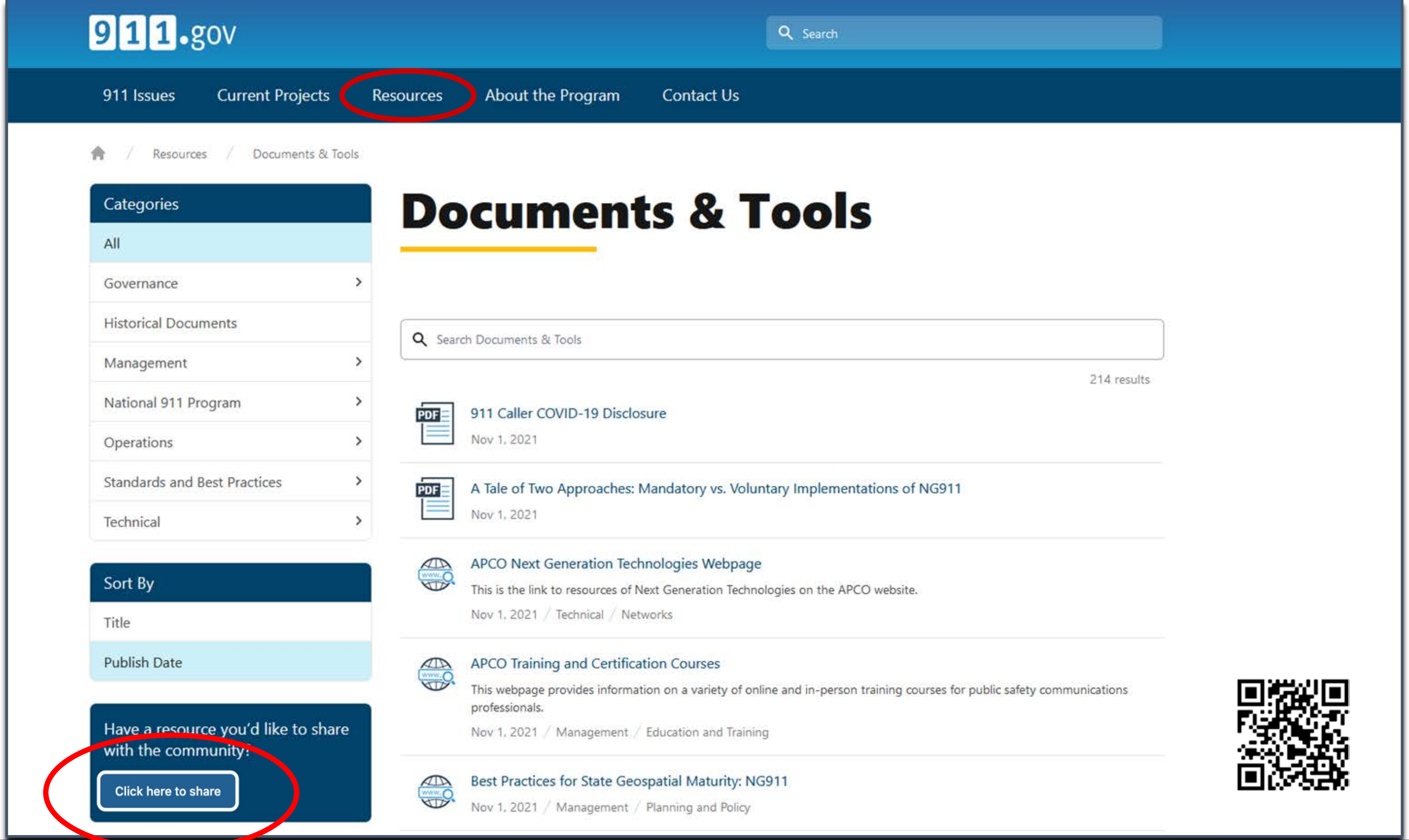
State of 911

Webinar Series

NATIONAL 911 PROGRAM
November 8, 2022

State of 911 Webinar Series

- Designed to provide useful information about federal and state participation in the planning, design, and implementation of Next Generation 911 (NG911) coupled with real experiences from leaders overseeing these transitions throughout the country
- Webinars are typically held every other month and include presentations from a federal-level 911 stakeholder and state-level 911 stakeholder, each followed by a 10-minute Q&A period
- For closed captioning, hover at the bottom of the Zoom screen for meeting controls, then click CC to start viewing closed captioning
- For more information on future webinars, to access archived recordings, and to learn more about the National 911 Program, please visit 911.gov
- Feedback or questions can be sent to: National911Team@MissionCriticalPartners.com



911.gov

Search

911 Issues | Current Projects | Resources | About the Program | Contact Us

Resources / Documents & Tools

Categories

- All
- Governance
- Historical Documents
- Management
- National 911 Program
- Operations
- Standards and Best Practices
- Technical

Sort By

- Title
- Publish Date

Have a resource you'd like to share with the community?

Click here to share

Documents & Tools

Search Documents & Tools

214 results

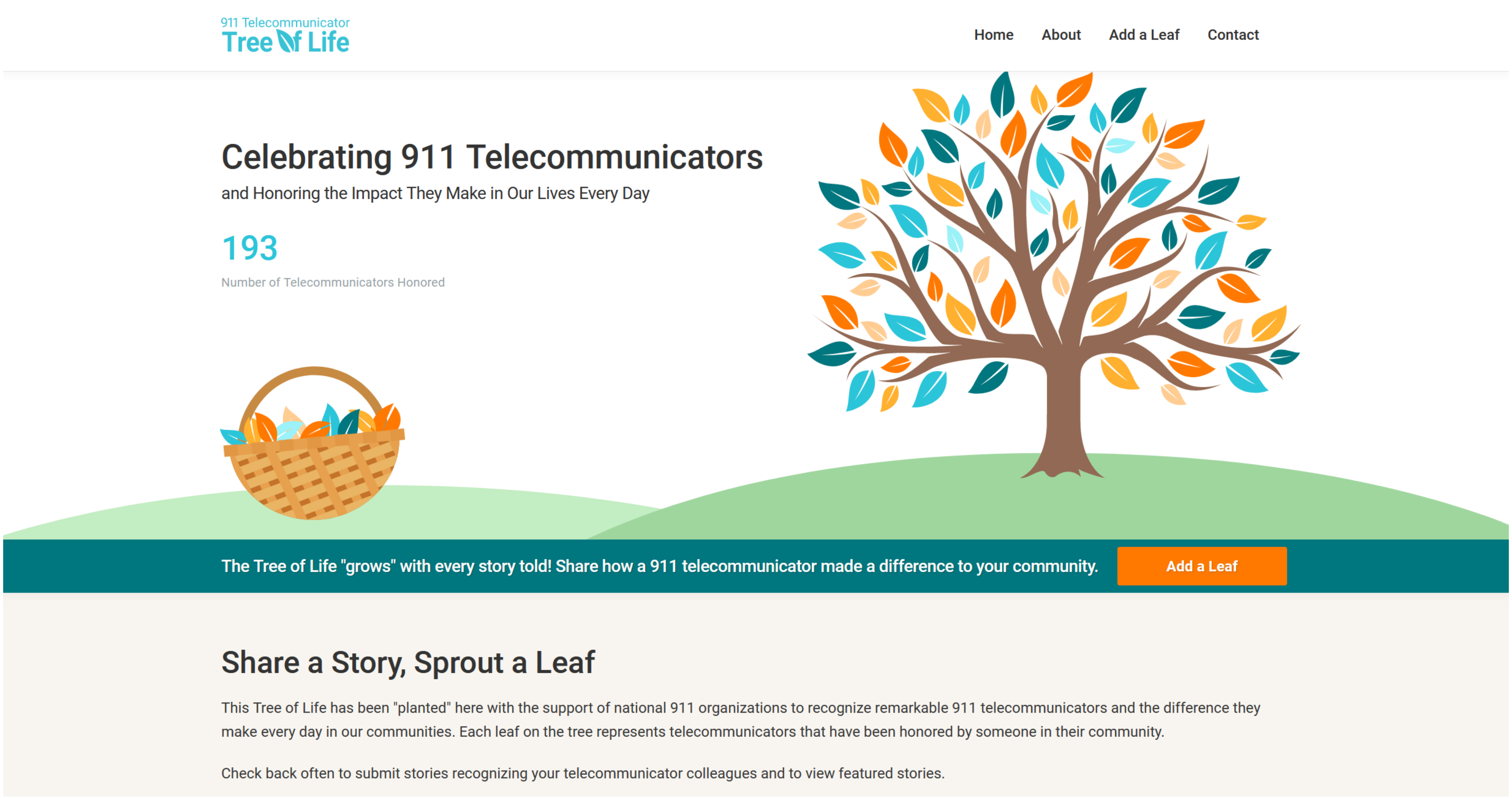
911 Caller COVID-19 Disclosure
Nov 1, 2021

A Tale of Two Approaches: Mandatory vs. Voluntary Implementations of NG911
Nov 1, 2021

APCO Next Generation Technologies Webpage
This is the link to resources of Next Generation Technologies on the APCO website.
Nov 1, 2021 / Technical / Networks

APCO Training and Certification Courses
This webpage provides information on a variety of online and in-person training courses for public safety communications professionals.
Nov 1, 2021 / Management / Education and Training

Best Practices for State Geospatial Maturity: NG911
Nov 1, 2021 / Management / Planning and Policy



Celebrating 911 Telecommunicators

and Honoring the Impact They Make in Our Lives Every Day

193

Number of Telecommunicators Honored

The Tree of Life "grows" with every story told! Share how a 911 telecommunicator made a difference to your community.

Share a Story, Sprout a Leaf

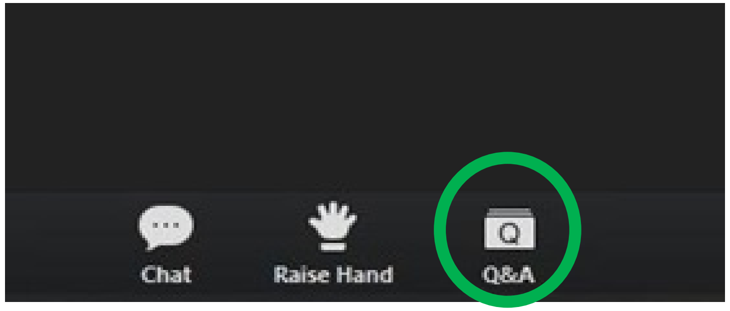
This Tree of Life has been "planted" here with the support of national 911 organizations to recognize remarkable 911 telecommunicators and the difference they make every day in our communities. Each leaf on the tree represents telecommunicators that have been honored by someone in their community.

Check back often to submit stories recognizing your telecommunicator colleagues and to view featured stories.

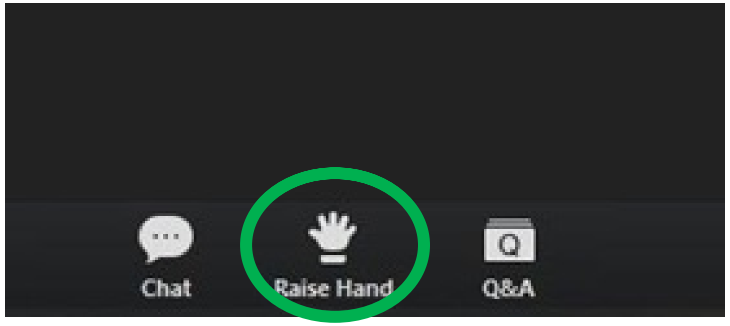
Questions

The "Q&A" feature is in the meeting controls that will display when hovering at the bottom of the Zoom screen.

Once clicked, a new pop-up window/chat box will open to navigate the Q&A functions.



Or, to ask your question "live," use the "Raise Hand" feature to request your phone line to be unmuted and you will be called upon to ask your question.



CYBER RESILIENT 911 (CR911) PROGRAM OVERVIEW

November 8, 2022

Cyber Resilient 911 (CR911)

An initiative to help 911 centers close the emerging operational cybersecurity gaps

911 at Risk

Cyber Incidents

47% Of Public Safety Answering Points (PSAPs)/Public Safety Communications Centers (PSCCs) indicated that cybersecurity incidents impacted their ability to communicate over the past five years

Cyber Planning

25% Indicated that they don’t have funding for cybersecurity operating or maintenance costs

38% Indicated their cybersecurity funding is insufficient to meet their needs

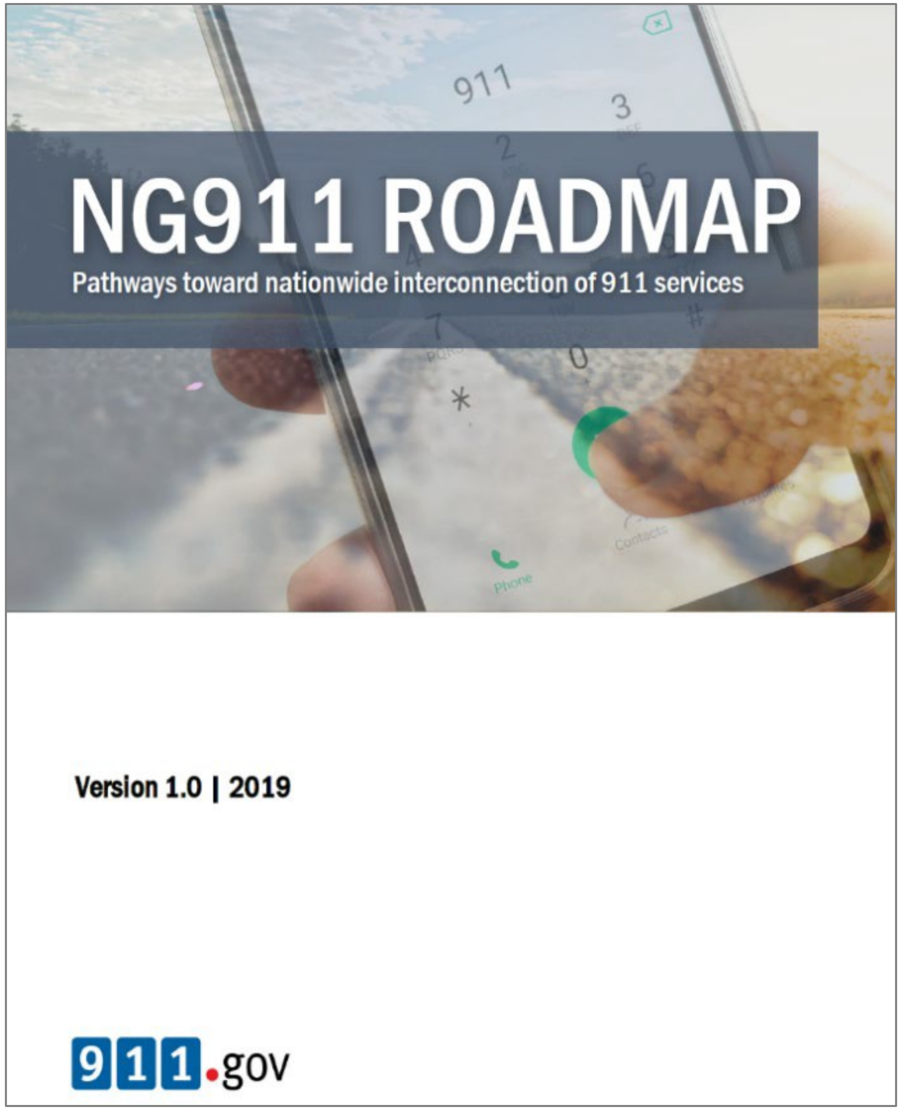
63% Indicated not having incident response plans, policies, and capabilities

65% Indicated not having a mitigation strategy in place

Data from the 2018 SAFECOM Nationwide Survey (SNS) Results. The SNS is a nationwide data collection effort to obtain actionable and critical data that drives the nation’s emergency communication policies, programs, and funding.

Congressional Directive

- “Enable a “resilient next generation 911 (NG911) ecosystem”
- In coordination with the the Federal Communications Commission (FCC), the National Highway Traffic Safety Administration (NHTSA), and the National Telecommunications and Information Administration (NTIA) to lay the groundwork
- Guided by recommendations from the National 911 Program’s NG911 Roadmap



NG911 ROADMAP

Pathways toward nationwide interconnection of 911 services

Version 1.0 | 2019

911.gov

Material & Non-Material CR911 Solutions

Education and Training

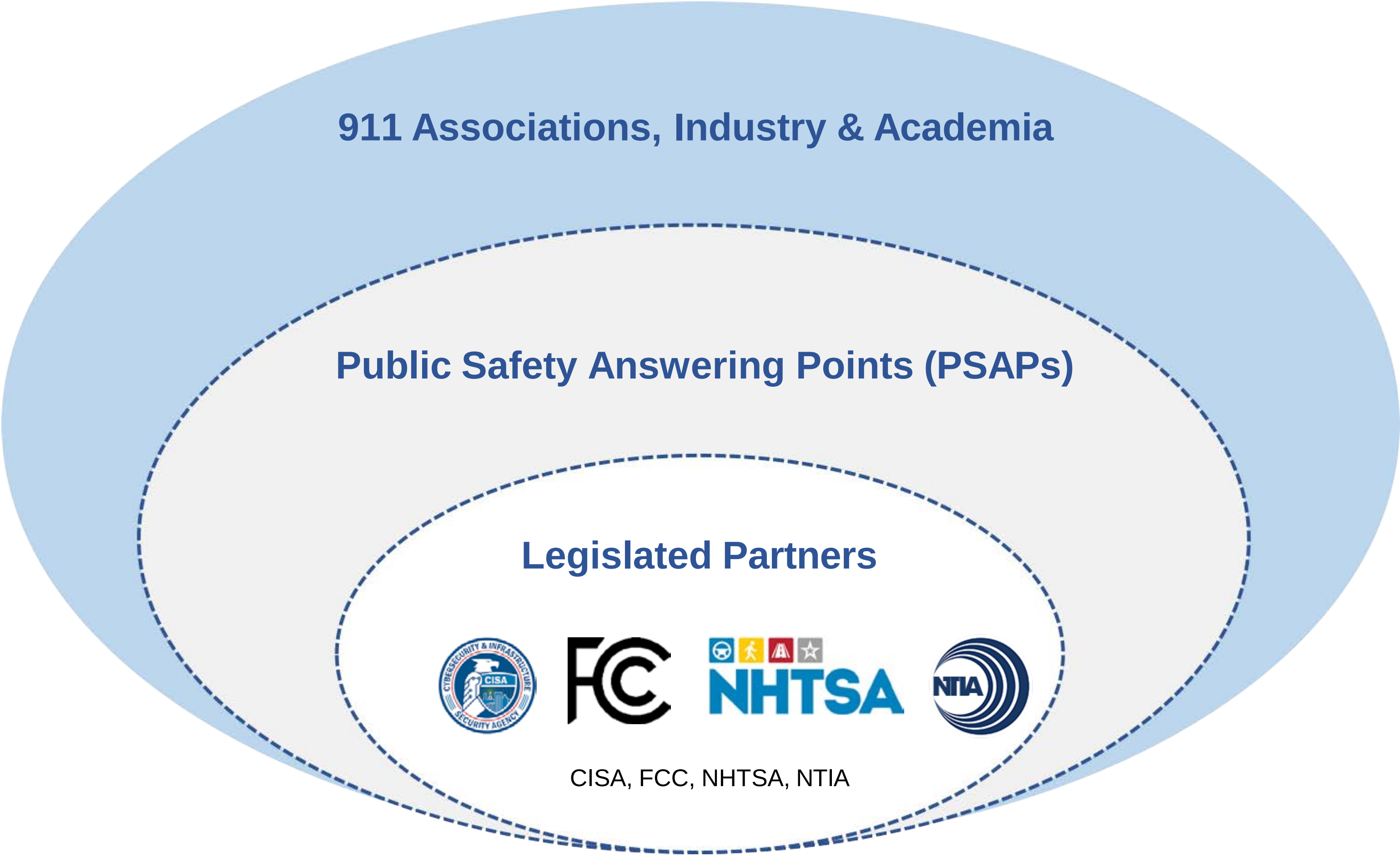
Cyber Risk Management

Potential Technical Solutions:

- *Cybersecurity as a Service*
- *Regional Ops Centers*

Stakeholder Engagement

Cyber Resilient 911 Stakeholders



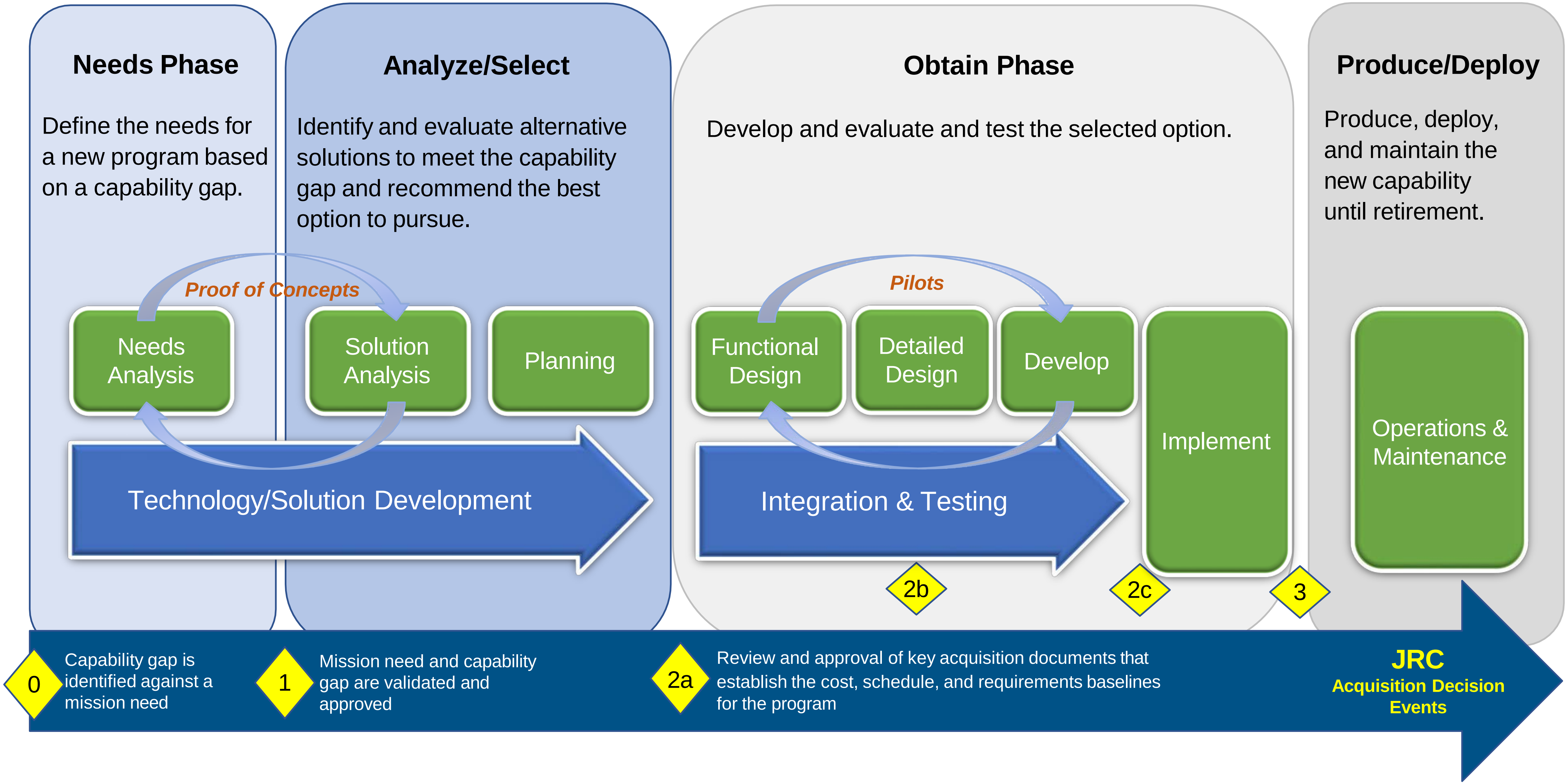
911 Associations, Industry & Academia

Public Safety Answering Points (PSAPs)

Legislated Partners

CISA, FCC, NHTSA, NTIA

Systems Engineering Lifecycle



Needs Phase

Define the needs for a new program based on a capability gap.

Analyze/Select

Identify and evaluate alternative solutions to meet the capability gap and recommend the best option to pursue.

Obtain Phase

Develop and evaluate and test the selected option.

Produce/Deploy

Produce, deploy, and maintain the new capability until retirement.

Proof of Concepts

Needs Analysis

Solution Analysis

Planning

Technology/Solution Development

Pilots

Functional Design

Detailed Design

Develop

Implement

Integration & Testing

Operations & Maintenance

2b

2c

3

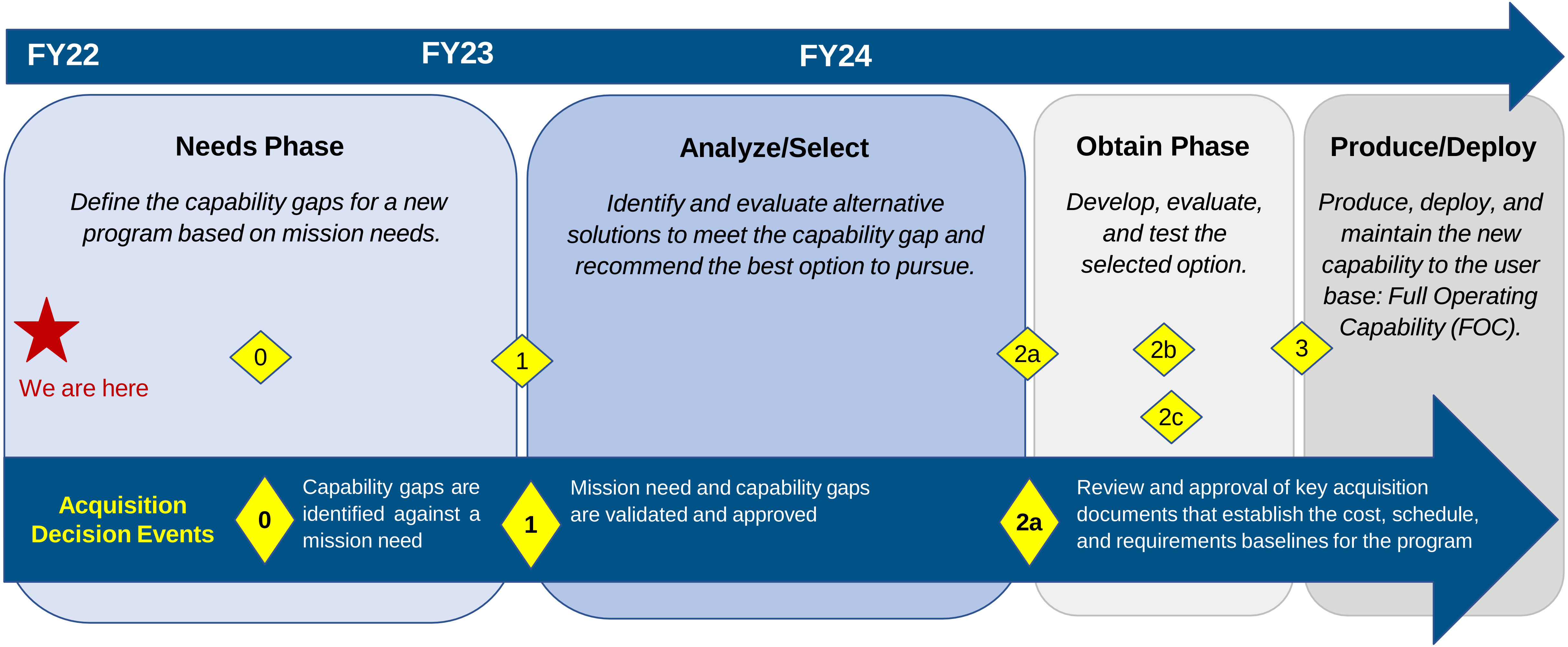
0 Capability gap is identified against a mission need

1 Mission need and capability gap are validated and approved

2a Review and approval of key acquisition documents that establish the cost, schedule, and requirements baselines for the program

JRC
Acquisition Decision Events

DHS Acquisition Process & Timeline



FY22 FY23 FY24

Needs Phase

Define the capability gaps for a new program based on mission needs.

Analyze/Select

Identify and evaluate alternative solutions to meet the capability gap and recommend the best option to pursue.

Obtain Phase

Develop, evaluate, and test the selected option.

Produce/Deploy

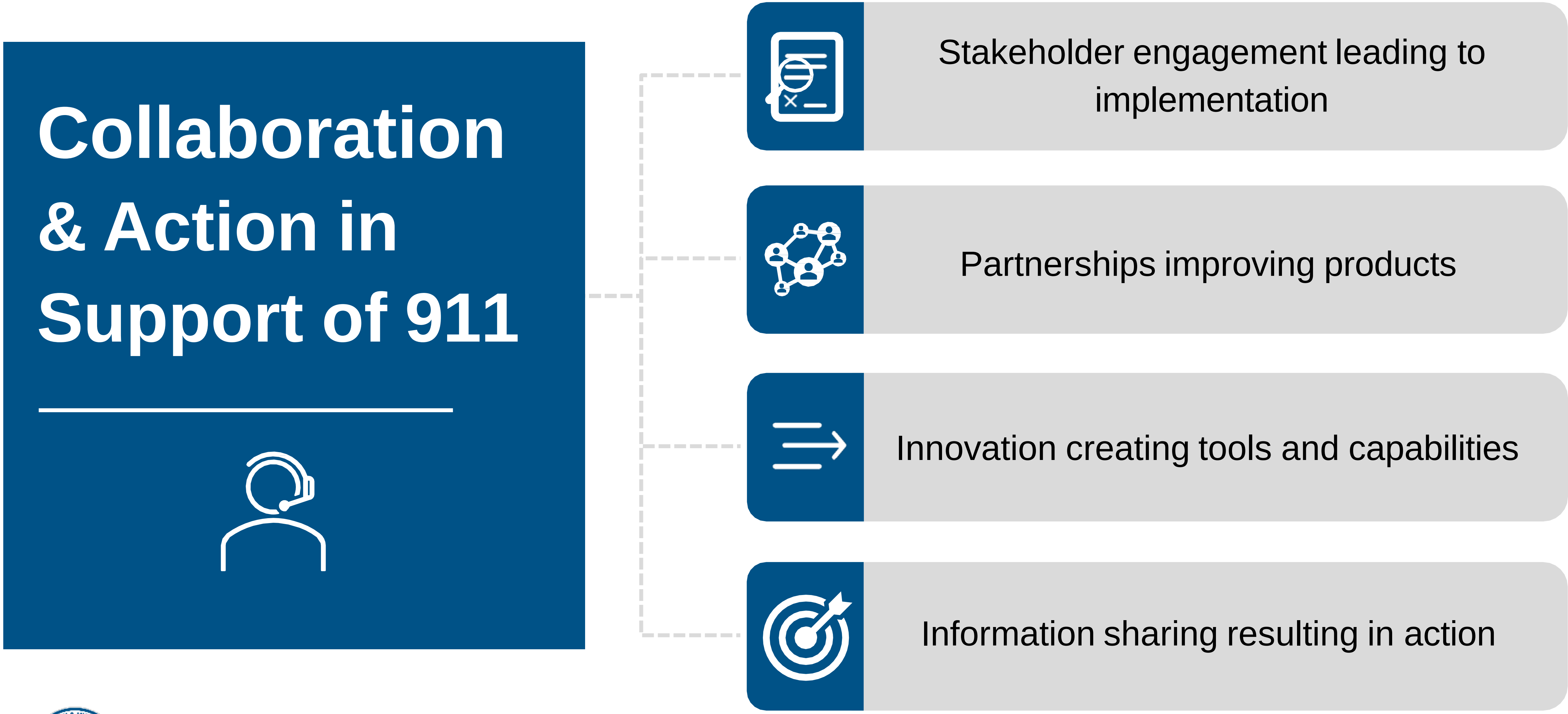
Produce, deploy, and maintain the new capability to the user base: Full Operating Capability (FOC).

Acquisition Decision Events

0 Capability gaps are identified against a mission need

1 Mission need and capability gaps are validated and approved

2a Review and approval of key acquisition documents that establish the cost, schedule, and requirements baselines for the program



Collaboration & Action in Support of 911

- Stakeholder engagement leading to implementation
- Partnerships improving products
- Innovation creating tools and capabilities
- Information sharing resulting in action

Facilitation of Forums

New Self-Assessment Tool Helps Identify Next Generation 9-1-1 Readiness

Next Generation 911 Incident-Related Imagery Impacts 101

Preparing Your 911 Center for Receiving Multimedia

MALWARE, TDoS, AND A STATE'S PERSPECTIVE

LESSONS LEARNED FROM 911 CENTERS

GIS Lifecyle Best Practices Guide for Next Generation 911

SAFECOM/NCSWIC
Next Generation 911 (NG911)
Working Group

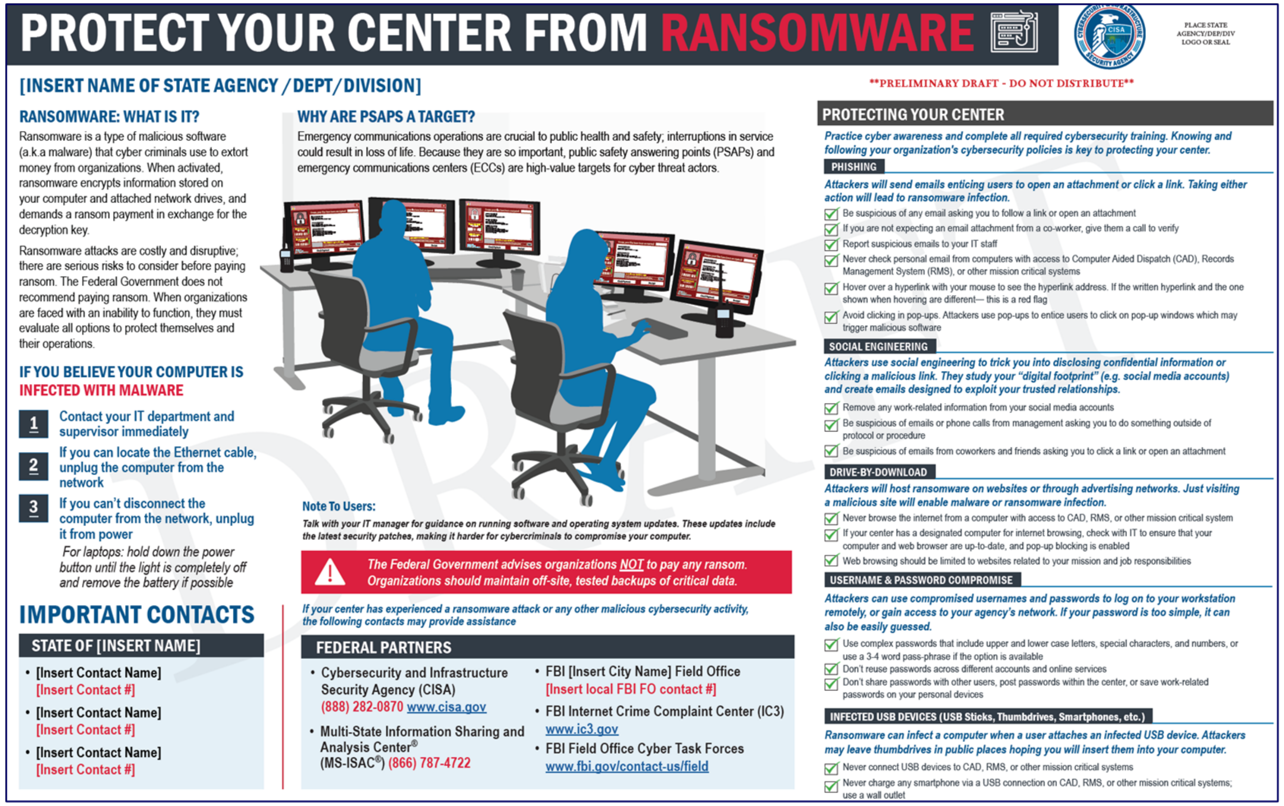
ECPC Federal 911
Working Group

Cybersecurity Research & Development

ECC Profile & Dashboard	Cyber-Resilient Public Safety Infrastructure	Telephony Denial of Service Mitigation	Multimedia Analysis
Assess and manage 911 center cybersecurity	Monitor ECC traffic for malicious activity	Enable viable defense and mitigation capability	Consume multimedia in the 911 system
Security control profile	Traffic monitoring capability	Detection capability with visualization dashboard	Multimedia analysis engine capability
Enhanced toolset to support assessment and management of ECC/public safety answering point (PSAP) cybersecurity	Improved capabilities to monitor ECC/PSAP traffic for anomalous and malicious activity	Enhanced toolset to support awareness and defense of cyber attacks	Improved analysis of multimedia content arriving at ECCs/PSAPs for relevance and cyber threats

Education & Training

- CISA Cyber Advisors, Resource Hub & Services Catalogue
- Ransomware Poster
- 911/PSAP Cyber Awareness & Assessment TA (webinar)
- Updates to core offerings:
  - ITSL
  - NIFOG 2.01
  - NSSE/SEAR Toolkit



PROTECT YOUR CENTER FROM RANSOMWARE

PLACE STATE AGENCY/DEP/DIV LOGO OR SEAL

[INSERT NAME OF STATE AGENCY / DEPT/ DIVISION]

PRELIMINARY DRAFT - DO NOT DISTRIBUTE

RANSOMWARE: WHAT IS IT?

Ransomware is a type of malicious software (a.k.a malware) that cyber criminals use to extort money from organizations. When activated, ransomware encrypts information stored on your computer and attached network drives, and demands a ransom payment in exchange for the decryption key.

Ransomware attacks are costly and disruptive; there are serious risks to consider before paying ransom. The Federal Government does not recommend paying ransom. When organizations are faced with an inability to function, they must evaluate all options to protect themselves and their operations.

IF YOU BELIEVE YOUR COMPUTER IS INFECTED WITH MALWARE

1. Contact your IT department and supervisor immediately
2. If you can locate the Ethernet cable, unplug the computer from the network
3. If you can't disconnect the computer from the network, unplug it from power

   For laptops: hold down the power button until the light is completely off and remove the battery if possible

WHY ARE PSAPS A TARGET?

Emergency communications operations are crucial to public health and safety; interruptions in service could result in loss of life. Because they are so important, public safety answering points (PSAPs) and emergency communications centers (ECCs) are high-value targets for cyber threat actors.

Note To Users:

Talk with your IT manager for guidance on running software and operating system updates. These updates include the latest security patches, making it harder for cybercriminals to compromise your computer.

⚠ *The Federal Government advises organizations NOT to pay any ransom. Organizations should maintain off-site, tested backups of critical data.*

IMPORTANT CONTACTS

If your center has experienced a ransomware attack or any other malicious cybersecurity activity, the following contacts may provide assistance

STATE OF [INSERT NAME]

- [Insert Contact Name] [Insert Contact #]
- [Insert Contact Name] [Insert Contact #]
- [Insert Contact Name] [Insert Contact #]

FEDERAL PARTNERS

- Cybersecurity and Infrastructure Security Agency (CISA) (888) 282-0870 www.cisa.gov
- Multi-State Information Sharing and Analysis Center® (MS-ISAC®) (866) 787-4722
- FBI [Insert City Name] Field Office [Insert local FBI FO contact #]
- FBI Internet Crime Complaint Center (IC3) www.ic3.gov
- FBI Field Office Cyber Task Forces www.fbi.gov/contact-us/field

PROTECTING YOUR CENTER

Practice cyber awareness and complete all required cybersecurity training. Knowing and following your organization's cybersecurity policies is key to protecting your center.

PHISHING

Attackers will send emails enticing users to open an attachment or click a link. Taking either action will lead to ransomware infection.

- ☑ Be suspicious of any email asking you to follow a link or open an attachment
- ☑ If you are not expecting an email attachment from a co-worker, give them a call to verify
- ☑ Report suspicious emails to your IT staff
- ☑ Never check personal email from computers with access to Computer Aided Dispatch (CAD), Records Management System (RMS), or other mission critical systems
- ☑ Hover over a hyperlink with your mouse to see the hyperlink address. If the written hyperlink and the one shown when hovering are different— this is a red flag
- ☑ Avoid clicking in pop-ups. Attackers use pop-ups to entice users to click on pop-up windows which may trigger malicious software

SOCIAL ENGINEERING

Attackers use social engineering to trick you into disclosing confidential information or clicking a malicious link. They study your "digital footprint" (e.g. social media accounts) and create emails designed to exploit your trusted relationships.

- ☑ Remove any work-related information from your social media accounts
- ☑ Be suspicious of emails or phone calls from management asking you to do something outside of protocol or procedure
- ☑ Be suspicious of emails from coworkers and friends asking you to click a link or open an attachment

DRIVE-BY-DOWNLOAD

Attackers will host ransomware on websites or through advertising networks. Just visiting a malicious site will enable malware or ransomware infection.

- ☑ Never browse the internet from a computer with access to CAD, RMS, or other mission critical system
- ☑ If your center has a designated computer for internet browsing, check with IT to ensure that your computer and web browser are up-to-date, and pop-up blocking is enabled
- ☑ Web browsing should be limited to websites related to your mission and job responsibilities

USERNAME & PASSWORD COMPROMISE

Attackers can use compromised usernames and passwords to log on to your workstation remotely, or gain access to your agency's network. If your password is too simple, it can also be easily guessed.

- ☑ Use complex passwords that include upper and lower case letters, special characters, and numbers, or use a 3-4 word pass-phrase if the option is available
- ☑ Don't reuse passwords across different accounts and online services
- ☑ Don't share passwords with other users, post passwords within the center, or save work-related passwords on your personal devices

INFECTED USB DEVICES (USB Sticks, Thumbdrives, Smartphones, etc.)

Ransomware can infect a computer when a user attaches an infected USB device. Attackers may leave thumbdrives in public places hoping you will insert them into your computer.

- ☑ Never connect USB devices to CAD, RMS, or other mission critical systems
- ☑ Never charge any smartphone via a USB connection on CAD, RMS, or other mission critical systems; use a wall outlet

SAFECOM®
NATIONWIDE SURVEY

COMING SOON

INFLUENCE THE FUTURE OF EMERGENCY COMMUNICATIONS

visit **cisa.gov/sns**
email **sns@cisa.dhs.gov**

CYBERSECURITY & INFRASTRUCTURE

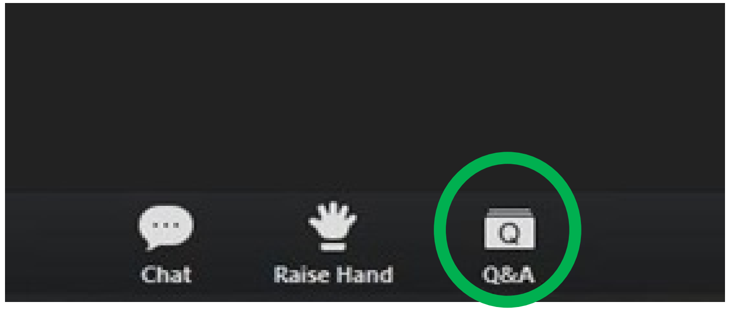
CISA

SECURITY AGENCY

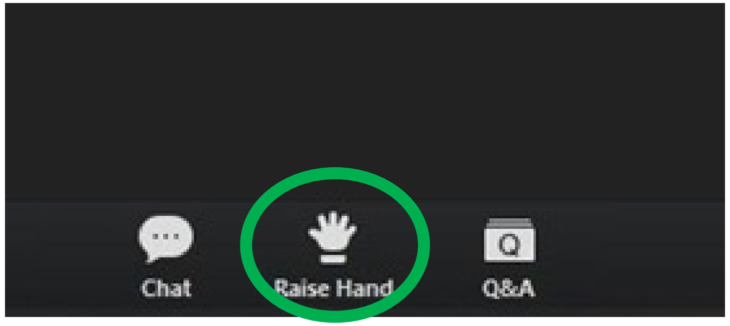
Questions

The “Q&A” feature is in the meeting controls that will display when hovering at the bottom of the Zoom screen.

Once clicked, a new pop-up window/chat box will open to navigate the Q&A functions.



Or, to ask your question “live,” use the “Raise Hand” feature to request your phone line to be unmuted and you will be called upon to ask your question.



Tackling 911 Staffing Challenges

ANN PINGEL

ANNE ARUNDEL COUNTY POLICE DEPARTMENT

Hiring Challenges

- History on the application process
- Pre-COVID received high numbers of applications
- Once COVID hit the application numbers decreased
- Post-COVID the application numbers were not increasing as expected
- Reviewed the process to determine what was missing

Hiring Challenges (continued)

- Application process before recruiter:
  - Job posting was open for 20 days
  - Pre-hire testing
  - Open houses

- Oral interviews
- Electronic Statement of Personal History
- Background investigations
- Conditional letter of employment
- Drug test

What Needed to be Changed

- Looking back at what worked and where we needed to go as a department
- Reviewed areas where we are losing applicants and why
- Who was doing the recruiting currently
- Ways to move forward

Hiring a Recruiter

- What are you looking for in a recruiter
- Compile a job description to include experience, compensation, hours
- Make a list of expectations and responsibilities

Responsibilities of a Recruiter

- The recruiter needs to have a good understanding of expectations
- Have a good working knowledge of the organization
- What are the organization’s recruiting needs and commitments
- Comprehend the position of a 911 Specialist
- Knowledge of the application process

Expectations

- What is main goal for the recruiter?
- Develop a system on tracking the applicants and their progress
- Community outreach
- Knowledge of the duties and the position(s)

Knowledge of the Organization

- Selection process being utilized by the organization
- Observe 911 Specialists to understand the position
- Minimum qualifications for the position
- What disqualifies an applicant

Recruiting Needs

- Knowledge of organization’s social media, announcements, open houses, advertising tools, flyers and/or banners
- Types of events to attend to advertise the position(s)
- When is the best time to reach out to applicants

Best Practices

- Recruiter needs to assist in advertising the position by creating banners, flyers, posting on social media platforms
- Attend community hiring events, local high school and college job fairs
- Partner with sworn police recruits and attend events

Best Practices (continued)

- Best time to contact applicants
- Host open houses for applicants
- Work with applicants regarding Critical testing and take Critical to understand the test
- Provide as much information to the applicants about the test as possible
- Go over background investigation and process with applicant
- Have knowledge of background software to work with applicants

Best Practices (continued)

- Keep lines of communication open with applicants to answer questions
- Talk to them about the oral interview and how to best prepare for the interview
- Set up the observations for the applicants
- Maintain communication with applicants until final offers are received
- Maintain records on past and current applicants to communicate about future hiring processes

QUESTIONS??

Contact Information

Ann Pingel

Communications Manager

Anne Arundel County Police Department

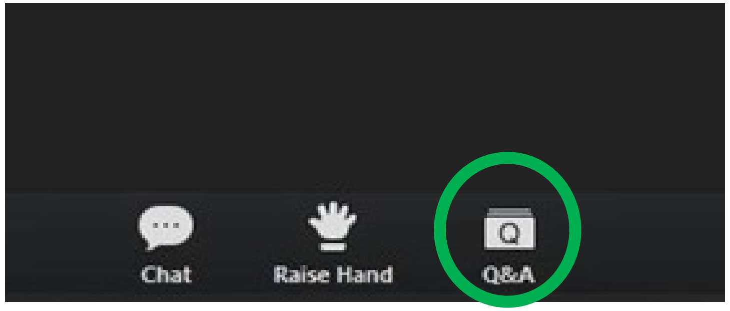
apingel@aacounty.org

410-222-8600

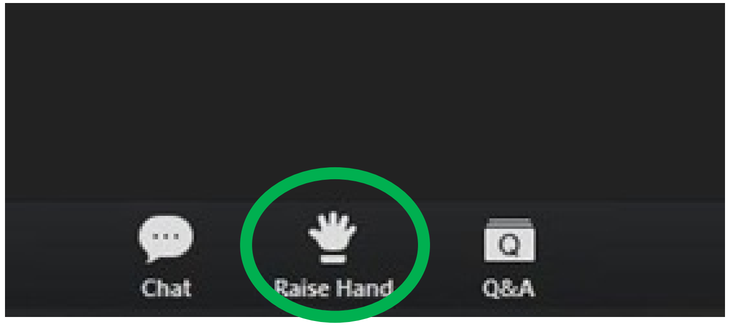
Questions

The “Q&A” feature is in the meeting controls that will display when hovering at the bottom of the Zoom screen.

Once clicked, a new pop-up window/chat box will open to navigate the Q&A functions.



Or, to ask your question “live,” use the “Raise Hand” feature to request your phone line to be unmuted and you will be called upon to ask your question.



Future Webinars

Stay tuned for a listing of the 2023 webinar dates

Previous State of 911 webinars are available at: www.911.gov/webinars.html

National 911 Program

- Brian Tegtmeyer

  National 911 Program Coordinator

  202-366-2705

  Brian.Tegtmeyer@dot.gov

- Feedback or questions can be sent to:
  National911Team@MissionCriticalPartners.com