TWO THINGS EVERY 911 CENTER SHOULD DO TO IMPROVE CYBERSECURITY

911 CYBER ATTACK SURFACES

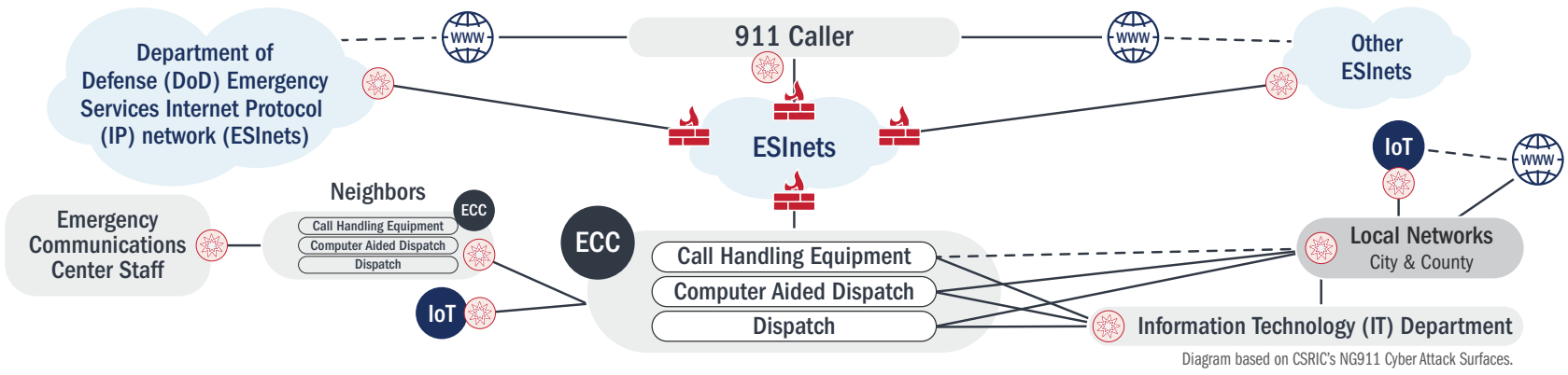

Diagram based on CSRIC's NG911 Cyber Attack Surfaces.

The nation's most direct route to emergency assistance, the 911 system, requires stable, safe, and resilient communications. Sophisticated criminal actors and nation-states exploit cyber vulnerabilities to threaten the delivery of essential services. The integration of new technology, such as multimedia, expands threat vectors, and increased interconnection of systems poses threats across a broader attack surface.

Cybersecurity is a shared responsibility. All organizations play a role, and some organizations are being required to comply with standards, such as the National Fire Protection Association's (NFPA) Standard for Emergency Services Communications (NFPA 1225), to improve cybersecurity posture. SAFECOM, the National Council of Statewide Interoperability Coordinators (NCSWIC), the Cybersecurity and Infrastructure Security Agency (CISA), the National Institute of Standards and Technology (NIST), and other partners have resources to help. Cybersecurity has become an integral part of mission function and operations for legacy and Next Generation 911 (NG911) systems. Working with others within the community, government, industry, and academia to establish consistent standards, policies, procedures, interoperability, and implementation guidance for NG911 deployment is crucial.

TWO THINGS EVERY 911 CENTER CAN DO TO REDUCE CYBER RISKS

CYBER RISK ASSESSMENT

Cybersecurity (cyber) risk assessments assist emergency communications centers (ECCs)/public safety answering points (PSAPs) in understanding vulnerabilities and threats to their operations (e.g., mission, functions, image, reputation), organizational assets, and individuals. A cyber risk assessment can help an ECC/PSAP determine next steps in protecting their systems and networks from malicious actors and infrastructure failures.

Below are resources that can help ECCs/PSAPs conduct cyber assessments:

- SAFECOM, *Guide to Getting Started with a Cyber Risk Assessment* (anticipated publication date October 2022)
- CISA, *Cyber Essentials Starter Kit: The Basics for Building a Culture of Cyber Readiness*
- CISA, *Public Safety Communications and Cyber Resiliency Toolkit*
- CISA, *Cyber Resiliency Resources for Public Safety Fact Sheet*
- NIST, *NIST Cybersecurity Framework*

CYBER INCIDENT RESPONSE AND VULNERABILITY RESPONSE PLANS

Cyber incident response and vulnerability response plans provide guidance on identifying, mitigating, responding to, and recovering from incidents that may impact ECC/PSAP systems and operations. It is key to ensure all users and devices, network infrastructure and connections, data, data applications, and services are fully assessed to prevent disruptions. An incident response plan is necessary to minimize gaps in services, prevent loss of data and services, and ensure continuity of operations. Vulnerability response plans address steps to follow regarding identified cybersecurity threats and vulnerabilities. It is essential to coordinate with stakeholders and service providers to develop joint mutual agreements on continuity of operations during a crisis to include cyberattacks. Recovering data, testing, and training are critical components to response plans, and coordination with all stakeholders and partners can assist in a smooth transition.

Below are resources that can help ECCs/PSAPs develop cyber incident response plans:

- CISA, *Federal Government Cybersecurity Incident and Vulnerability Response Playbooks*
- CISA, *Essential Elements: Your Crisis Response*
- CISA, *Cyber Alerts*
- CISA, *Cyber Incident Response*

HOW CAN OUR ECC/PSAP PARTICIPATE?

Perform regular cyber risk assessments and based on the findings:

- Develop incident and vulnerability response plans, recovery plans, and continuity of operations (COOP) plans to assist in cybersecurity incident response
- Exercise plans so they can be validated, refined, and updated
- Incorporate lessons learned into recovery planning processes and strategies
- Train response personnel on the latest security, resiliency, COOP, and operational practices and maintain in-service training as new technology and methods are made available
- Maintain coordination and communication with other partners, vendors, and stakeholders such as the Statewide Interoperability Coordinator (SWIC)
- Coordinate with service providers when developing and updating cyber response plans
- ECCs/PSAPs should consider implementing cyber threat detection and mitigation capabilities and using resources such as CISA capabilities and fusion centers. These state and local centers may provide system monitoring, threat identification, and intelligence sharing, allowing ECCs/PSAPs to maintain a proactive cyber posture
- Become familiar with Cyber Incident Response Case Studies and understand and prioritize threats that impact the agency's mission
- Consider implementing NG911 which maintains advanced authentication and enhanced security capabilities

ADDITIONAL CYBERSECURITY RESOURCES

For more information on this and other cybersecurity initiatives, contact ng911wg@cisa.dhs.gov or visit cisa.gov/safecom/next-generation-911 and cisa.gov.