KARTHIK CONSULTING
Beyond the expected

3120 Fairview Park Drive
Suite 800
Falls Church, VA 22042
www.karthikconsulting.com

AT A GLANCE

Cybersecurity for Nationwide 9-1-1 Critical Infrastructure Emergency Communications Systems

CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE
A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Science and Technology

KEY STATS

- As the Principal Investigator (PI), conducted a macro level cybersecurity assessment of legacy/NG911 Public Safety Answering Point (PSAP) & legacy/NG911 PSAP technical architecture.
- Created the “PSAP Profile” as a curated set of cybersecurity controls based on NIST SP800-53A and aligned the PSAP profile with the Cyber Security Framework (CSF),
- Supported the implementation of the PSAP Profile in DHS funded Cyber Secure Dashboard (CSD) tool.
- Following a consultative assessment methodology, conducted Pilot assessments of PSAPs using the PSAP Profile, to develop the risk profile of PSAPs across the country and document their cybersecurity posture.
- Published an updated PSAP Profile for cybersecurity interoperability of NG911 PSAPs

KC CUSTOMER IN FOCUS:
Through a joint effort between CIRI, University of Illinois, DHS Science & Technology, and CISA Offices, KC led a comprehensive research project to identify and develop best practice solutions around improving the cybersecurity posture of the U.S 9-1-1 Critical Infrastructure Emergency Communications System.

SIGNIFICANCE OF REQUIREMENTS:
The national 911 system is an essential part of the critical infrastructure of the United States. It is intertwined to our national security fabric and offers reach and comfort of emergency public and medical security and safety to all. DHS recognizes the 9-1-1 Public Safety Answering Points (PSAP) as part of the nation’s critical functions of its Critical Infrastructure, and one that is to be protected from cyber-attacks.

The core objective of this requirement was to enhance the security and resilience of the nation’s 9-1-1 system. KC led the advancement of this important initiative first through a cyber security assessment of the of the nation’s 9-1-1 PSAPs, especially as the nation transitioned from an analog based 9-1-1 system to the next generation digital and IP-based connected 9-1-1 system. All PSAPs were placed on a spectrum from legacy to next-generation 9-1-1 (NG911) systems. Legacy systems refer to an old style of telephone system that many users likely think of when they picture an emergency call center. On the other end of the spectrum are NG911 centers, which are working to integrate text and video into emergency communications. Through this KC led research initiative, the NIST CSF and SP 800-53A based PSAP Profile was developed to assess the cybersecurity posture of the PSAPs/9-1-1 systems.

Continued on next page

A hack into the PSAP system could take down the emergency network altogether or send false information to the public or emergency responders. While an attack affecting the call system could be devastating, the cybersecurity framework developed by the CIRI team would also need to cover the internal and external communications of employees to make sure a hacker couldn't break into the computer network. Telephone Denial-Of-Service (TDOS) attacks on the legacy 9-1-1 system have already occurred. This attack vector came in via wireless networks, channeled via a social media and internet sites; proving that the existing legacy system is vulnerable, and cyber-risk is real, and present. Ransomware has also been used extensively against public safety networks.

CISA Emergency Communications Division (ECD) and the Emergency Public Safety Sector, and more specifically, PSAPs across the nation are intended to be the primary beneficiaries of this project.

While transitioning to NG911 is a primary goal, currently no PSAPs across the country have completely reached this milestone. Most 9-1-1 centers are currently operating under a "hybrid" model, somewhere between legacy and NG911. KC and our research partners are actively working to complete this systems transition process and (over time) will have updates to this report to share progress.

OPPORTUNITIES FOR KC IMPACT:

Proposed criteria for categorizing and developing a curated "PSAP Profile", using the NIST SP 800-53A controls and Cyber Security Framework (CSF) to measure and track the cybersecurity posture of PSAPs.

Conducted consultative PSAP profile based "pilot" assessments of PSAPs.

As the PSAP threat landscape rapidly changes so does the urgency to secure and improve this critical infrastructure. This project addresses the Goals and Objectives identified in the CISA Strategic Intent document (published in August 2019) by proposing to enhance the current and ongoing security and resilience of the PSAP ecosystem.

DELIVERED RESULTS:

- Phase 1 research of PSAPs completed and final report published.
- PSAP Profile published and approved by CIRI/CISA/DHS S&T.
- PSAP profile implemented in the Cybersecure Dashboard tool.
- PSAP Profile based "Pilot" assessments completed.
- Phase 2, further research to understand the unique requirements of PSAPs migrating to NG911 completed.

KEY AREAS OF KC IMPACT:

Used NIST CSF and relevant SP800-53 R4, SP800-39, SP800-37 security controls and tools to conduct a macro level cyber-vulnerability and gaps assessment and analysis of typical PSAP architecture of various PSAP categories.

- Tailored best practices guidance to match the size/complexity of the diverse PSAP eco-systems, including those in transition to NG-911.
- Conducted literature review to determine the edge contours of current state of research and practice.
- Developed interview and technical assessment instruments.

Continued on next page

AT A GLANCE *(continued)*

- Formed 9-1-1 Stakeholder Working Group to guide the effort and offered best-in-class cybersecurity and risk management expertise.
- Analyzed gaps, develop assessment report and proposed criteria for categorizing, developing cybersecurity best practices and CSF based profiles for PSAPs, using the CSD tool
- Conducted further research on PSAPs migrating to NG911 and updated the PSAP risk assessment profile to address cybersecurity interoperability risks.
- Conducted consultative assessments of PSAPs to examine and assess a range of technical and non-technical controls.
- An evaluation of the present cybersecurity state was conducted using the range of controls for plans, networks, architecture, data flow and inventory and policy, plans and procedures.
- Assessment and architecture analysis resulted in an assessment report and best practices set of recommendations, which has been embodied as part of a CSF based PSAP Profile via the DHS funded Cyber Secure Dashboard (CSD) tool.
- Working with CIRI and the CSD vendor to help obtain FedRAMP Accreditation for the CSD tool allowing it to be adopted as the repository to track the cybersecurity posture of all PSAPs

ABOUT US

Karthik Consulting was founded in 2008 to be a reliable and trusted advisor for our customers, providing independent, unbiased, and proven solutions that mitigate risk and help solve enterprise-wide IT challenges.

Our Cyber Security, Software Development and Program Management focus areas (and work methodology) ensure that we can deliver not just solutions, but architecture that scales and grows with the customer's needs over time. We are able to assist in projects ranging from short advisory engagements to assembling a full team to deliver a solution from concept through implementation and on-going management. KC has access to industry experts in various technologies and teaming partners to meet any of your IT challenges. The vision of KC is to bring the innovation, passion and agility of the commercial IT industry to meet the unique challenges of the federal government. We are a DOD Cleared Facility with a DCAA-approved accounting system.

CONTACT
Felix Martin, 571 435 7632
fmartin@karthikconsulting.com

CAGE: 56GH3
DUNS: 828199880
UEI: FGNNM7KNUPF6

PRIME CONTRACT VEHICLES:
GSA STARS III 8(a)
GSA MAS
GSA OASIS Pool 1 and 3
NIH CIO-SP3 8(a) & SB
Air Force SBEAS
Army RS3
Navy Seaport-NexGen
FAA eFAST

afaq ISO 20000-1 IT Service Management AFNOR CERTIFICATION

afaq ISO 27001 Information Security AFNOR CERTIFICATION

aws partner network Select Consulting Partner Public Sector Partner

ISO 9001:2015 CERTIFIED COMPANY PRI Registrar PERFORMANCE REVIEW INSTITUTE

ML3 CMMI APPRAISED DEV | SVC