CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

Protecting the nation's 911 system from cyber threats Present and Future

PI - Karthik Balasubramanian
Karthik Consulting, LLC

Project Overview

- **Utilize NIST cybersecurity standards and tools to:**
  - Conduct a macro level cybersecurity assessment of legacy/NG911 PSAP & legacy/NG911 PSAP technical architecture
  - Propose criteria for categorizing, developing cybersecurity best practices and Cyber Security Framework (CSF) based profile for PSAPs, integrate the PSAP CSF Profile into the DHS-developed Cyber Secure Dashboard (CSD) tool
- **Project Abstract and Objectives**
  - The national 911 system is an essential part of the critical infrastructure of the United States. DHS recognizes the 911 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 project is to enhance the security and resilience of the nation's 9-1-1 system. It is an essential part of the nation's critical infrastructure and spans several National Critical Functions that all in the US depend on for their safety and security. We intend to advance this with a cyber security assessment of the hybrid status of the nation's 9-1-1 PSAPs, especially as the nation transitions from an analog based 9-1-1 system to the next generation digital and IP-based connected 9-1-1 system.

Project Approach

Describe the overall project approach

- Conduct literature review to determine the edge contours of current state of research and practice
- Form 911 Stakeholder Working Group to guide the effort and offer expertise, select PSAP sites and manage risk
- Develop interview and technical assessment instruments
- Data acquisition and interviews of select PSAP personnel
- Use 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.
- Analyze gaps, develop assessment report and propose criteria for categorizing, developing cybersecurity best practices and CSF based profiles for PSAPs, using the CSD tool
- Tailor best practices guidance to match the size/complexity of the diverse PSAP eco-systems, including those in transition to NG-911

Testing Plan

Demonstrate that the project includes an appropriate and sound testing, evaluation, and validation plan to prove research results

- A comprehensive Site Survey plan has been published using NIST CSF, SP800-53 R4, SP800-37, SP800-39 standards and controls to examine and assess the gaps in networks, and a range of technical and non-technical controls. This includes governance, architecture and process of the system, environment, applications and services
- An evaluation of the present cybersecurity state will be conducted using the range of controls for plans, networks, architecture, data flow and inventory and policy, plans and procedures
- Validation of the provided documentation and adherence to various controls will be conducted via interviews and site visits.
- The research results will help create a set of actionable recommendations

Describe the project's defined metrics or targets and their appropriateness/relevancy for the stated project goal

- The project metrics includes a cybersecurity analysis of 3 PSAP sites, whereas the project team is pursuing 5 PSAP sites
- This assessment and architecture analysis will result in an assessment report and best practices that will be embodied as part of a CSF PSAP Profile via the DHS funded Cyber Secure Dashboard tool.
- This will deliver against the project goal of increasing cybersecurity of 911 sites, as this can be productized and operationalized for execution across the nation's PSAP sites

Milestones and Accomplishments

List the outcomes the research has achieve to date.

- PSAP assessment technical instruments finalized
- 5 PSAP sites selected and site surveys sent out to PSAPs
- Literature review complete

What major milestones need to be achieved for the project to reach its objectives.

- Conduct PSAP site assessments
- PSAP Assessment Analysis
- Draft Project Assessment Summary
- Final PSAP CSF Profile & Report

Discuss any impediments or obstacles that have hindered progress, and any mitigation strategies that have been put into place.

- COVID-19 situation has impacted PSAPs ability respond in a timely manner and has delayed site visit plans
- Planning to move to virtual visits based on response to site surveys and documentation provided

Project Impact

Demonstrate that the project addresses a knowledge gap that is important to the HSE and the value of the research.

- As the PSAP threat landscape rapidly changes so does the urgency to secure and improve this critical system. 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
- Create a more secure nation-wide PSAP system through the NIST CSF based Profile and map to cybersecurity controls. The CSD Profiles will be an actionable tool for the PSAPs to use to evaluate their cybersecurity posture against the NIST standards

Discuss which components benefit or could benefit from the research outcomes.

- The Emergency Communications Division (ECD) within the Cybersecurity and Infrastructure Security Agency (CISA) is identified as the DHS Champion
- Mr. David Nolan is the champion for this project. Several DHS S&T government program managers are actively participating in the Stakeholder Working Group guiding the research efforts to meet needs of the HSE
- The overall Emergency Public Safety Sector and more specifically PSAPs across the nation that are part of the HSE are intended to be the primary beneficiaries of this project

Also include how many students are involved and how they are integrated into the project.

- Student researchers from UIUC and Old Dominion University (ODU) are providing the literature review for this project

Transition Plans

Describe who is involved with ensuring the transition (e.g. acquisition, finance, information technology, intellectual property) and their roles and activities.

- Once the PSAP profiles are created KC and Heartland will engage with their IT, legal and finance teams to discuss transition details

Discuss the end users and customers of this research and how they are engaged. (specific mechanisms used for engaging with potential customers).

- The 5 selected PSAPs and their stakeholders are engaged in interviews discussing their technical implementation, policies and processes.
- Dissemination of the proposed PSAP profiles through implementation in the DHS funded Cyber Secure Dashboard tool

Indicate if there any commercialization entities need to realize the product/ service in the market.

- Work with CIRI/Heartland Institute to commercialize the PSAP specific profiles and create a market offering around it
- The 6000+ PSAPs and the 1000+ federal PSAPs are entities that can benefit from the cyber secure dashboard profiles to help understand and track their cybersecurity posture and risks.