GUAM POWER AUTHORITY
ATURIDÅT ILEKTRESEDÅT GUÅHAN
P.O.BOX 2977 • HAGÅTÑA, GUAM U.S.A. 96932-2977

FOR IMMEDIATE RELEASE

NOVEMBER 10, 2022

FOR MORE INFORMATION CONTACT:
JOYCE N. SAYAMA
COMMUNICATIONS MANAGER
PHONE NO.: (671) 648-3145

GPA CONDUCTS VULNERABILITY OF INTEGRATED SECURITY ANALYSIS (VISA) IMPLEMENTATION WORKSHOP FOR EMPLOYEES

Training provides tools and knowledge of the VISA and Design Basis Threat Methodologies

GPA employees joined by liaisons from the Guam Police Department and the US Department of Homeland Security completed the 5-day Electricity-Information Sharing and Analysis Center's (E-ISAC) Vulnerability of Integrated Security Analysis (VISA) Workshop held from August 22 - 26, 2022. The VISA is a cost-effective methodology that relies on Subject Matter Expertise input to help determine overall Physical Protection System effectiveness. The security-focused analysis approach utilizes the Design Basis Threat (DBT) as a reference in assessing the security of bulk power system physical infrastructure. The 32-hour workshop provided invaluable VISA methodology and DBT training for the participants, ultimately contributing to improvements in the Authority's Physical Security posture and its readiness to keep employees, assets, information, and the Island-wide Power System secure.

“The VISA and DBT methodology are critical tools to the Guam Power Authority's overall security management. I am grateful to E-ISAC, DHS and local law enforcement for their participation and efforts to keep Guam's power grid safe and secure,” said GPA General Manager, John M. Benavente, P.E. “Over the years we have made great strides with our security posture and security hardening projects as a critical infrastructure, and want to keep the momentum and continued shift in the security cultural change,” GM Benavente added.

The VISA workshop was facilitated by two trainers from E-ISAC and was designed to teach those attending how to effectively assess the vulnerability of a site’s critical assets. Being able to recognize security threats and developing the skills needed in order to combat these threats is significant in the overall security of GPA’s workforce. It is important for any government organization to prepare their staff as much as possible for these incidents, and in attending the workshop, the staff were taught how to develop plans and come up with viable scenarios to ascertain trouble spots in the security, and in turn, make better informed risk-based decisions based on these lessons.

Attendees that participated also had topic discussions on site characterization, target prioritization, onsite and offsite response timelines, and system effective analysis (SEA), to name a few. The workshop had an agenda open for further discussion on DBT, other security concerns, and the overall security environment for electrical utilities.

GPA Employees receiving certifications of completion for Vulnerability of Integrated Security Analysis (VISA) Implementation Workshop.

Front Row, Left to Right: Roel Cahinhinan, Engineer Supervisor; Jerald Guzman, Facilities Manager; Jeam Diaz, Asst. Plant Superintendent; Nanette Alger, Engineer III; Taryn Guzman, Personnel Specialist IV; Angela Balajadia, Inventory Management Officer; Beatrice Limtiaco, Asst. General Manager of Administration; Michelle Chargualaf, Management Analyst; George Charfauros Jr., Management Analyst; John Benavente, General Manager

Back Row, Left to Right: Irwin Loyola, Engineering Supervisor; Isaac Cruz, Plant Maintenance Supervisor, Bart Cruz, Engineer III; Melinda Mafnas, Asst. General Manager of Operations; Anselmo Manibusan, Manager of T&D; Melvyn Kwek, Chief Information Technology Officer; Alexander Salomon, Engineer III; Joshua Jimenez, Warehouse Supervisor II; Francisco Santos, Manager of Power Systems Control Center; Brandon Eusebio, Engineer I; Ed Leon Guerrero, Asst. Manager of T&D; Daniele Reyes, Buyer II

Not shown on photo: Edward Villanueva, Building Maintenance Supervisor; Frankie Quintanilla, Control Operator; Jessica Lazatin, Engineer III; John R. Alilin, Engineer; Jonathan Chargualaf, Network Systems Administrator; Joshua Lujan, Plant Maintenance Supervisor; Kenneth Gutierrez, Safety and Physical Security Manager; Pedro Sanchez, Management Analyst III; Vincent Sahagon, Substation Electrician Supervisor; Virgil Sana, Communication/Elect Tech; Rob Seifken, E-ISAC Facilitator; Ross Johnson, E-ISAC Facilitator

##

TLP:WHITE - Disclosure is not limited

Vulnerability of Integrated Security Analysis (VISA) Implementation Workshop

Purpose

The VISA Implementation Workshop is designed to teach participants how to optimize and use the VISA methodology in order to effectively assess the vulnerabilities of a site's critical assets. This methodology will provide the necessary framework and tools for asset owners and operators to make informed *risk-based* and *cost effective* decisions on the effectiveness of their physical protection systems (PPS), as well as provide justification to support targeted upgrades. This workshop also provides a unique opportunity to collectively engage and partner with other critical players involved who are also responsible for the protection of these critical assets, and provide a fundamental understanding of each person's critical role during a security incident.

Things to consider:

- Can you mitigate the threat you should be protecting against?
- How much risk are you willing to accept?
- Will proposed security upgrades mitigate the threat?
- Are you integrating realistic law enforcements response time into your assessments?

Workshop Training Objectives

- Understand and effectively use the methodology described in the VISA Implementation Guide to determine the overall system effectiveness of the PPS against a Design Basis Threat.
- Develop realistic and credible scenarios to describe attacks against real assets.
- Gain insight into site-specific critical pathways, weaknesses, vulnerabilities and the overall system effectiveness against a given threat.
- Determine and assess each layer of the PPS using the scenarios to make informed risk-based decisions on cost-effective and targeted upgrades with justification for funding.
- Integrate and effectively apply the operating principles of Detect, Assess and Respond into the initial security design for critical assets and infrastructure.
- Train participants so they are able to use this methodology wherever and whenever needed.

Logistics

- The host organization will provide a site to be used as a training aid.
- The in-person workshop is conducted over a four-and-a-half-day period and includes a site visit. A virtual workshop option is available.
- Class size: 20-30 people
- Target audience: Threat-Vulnerability Assessment personnel (outsider and insider threats), Security Managers, Operations Managers, Risk Managers, Facility/Site Manager(s), Security Operations Center (alarm management), Onsite/Offsite response (highly recommended), Intrusion Detection System (IDS) and Access Control systems technician.
- All participating non-host entity personnel will sign a non-disclosure agreement.

How To Get Involved

For more information on hosting a VISA Workshop, or simply learning more about the DBT or VISA IG, contact the E-ISAC at PhysicalSecurity@eisac.com.