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

PETITION

The Guam Power Authority hereby petitions the Consolidated Commission on Utilities (CCU) the following:

CREATION OF POSITION
Information Security Analyst I
Information Security Analyst II
Network Systems Technician I
Network Systems Technician II

This petition is in compliance with 4 GCA, Chapter 6, §6303 (d) (added by Public Law 28-112). The petition is also required by 4 GCA. §6205 and §6303 as public documents for the purposes of 5 GCA, Chapter 10, Art. 1 (Sunshine Law).

For more information, please visit the Guam Power Authority's website at https://www.guampowerauthority.com/corporate/human-resources/petitions. You may also contact GPA's Human Resources Office at 671-648-3130.

JOHN M. BENAVENTE, P.E.
GENERAL MANAGER

STAFF REPORT
CREATION OF POSITIONS -
INFORMATION SECURITY ANALYST I & II;
NETWORK SYSTEMS TECHNICIAN I & II;

I. REQUEST:

The and the Guam Power Authority (GPA) petitions the Consolidated Commission on Utilities (CCU) to create the following positions in the classified status in accordance with Public Law 28-112;

- Information Security Analyst I
- Information Security Analyst II
- Network Systems Technician I
- Network Systems Technician II

II. AUTHORITY:

Public Law 28-159, Section 3(c) Amendment of Certified, Technical and Professional Positions. The following information is provided pursuant to 4 GCA, §6303 (d) Creation of positions in the Autonomous Agencies and Public Corporations:

1. The petition of any agency, department, or public corporation listed in 4 GCA, §4105(d) of this Title to create a position shall include:

A. *The justification for the new position:*

The continued evolution of the cybersecurity landscape, coupled with GPA's increasing reliance on digital and network-dependent systems, has fundamentally changed the operational risk profile of the Authority. The rapid acceleration of digitalization during and after the pandemic has expanded GPA's technology footprint across enterprise systems, communications infrastructure, and operational support functions, thereby increasing exposure to cyber threats, system vulnerabilities, and service disruptions. These risks are further compounded by Guam's strategic geographic location and the heightened potential for targeted attacks on critical infrastructure. As a public utility, GPA must maintain uninterrupted, reliable service; therefore, the ability to proactively monitor, secure, and maintain its network and information systems is no longer supplemental—it is mission-critical. Establishing the Information Security Analyst I & II and Network Systems Technician I & II classifications ensures that the Authority has the dedicated, specialized workforce necessary to safeguard its systems, respond to incidents, and sustain operational reliability in an increasingly complex threat environment.

In addition to addressing operational risk, the creation of these positions is essential to resolving workforce limitations and strengthening internal capacity. Current Government of Guam classifications are either too broad or require fully qualified experience at entry, limiting GPA's ability to recruit and develop talent within a highly competitive and constrained labor market. The proposed tiered structure is intentionally designed to create a sustainable pipeline, allowing the Authority to hire at the entry level, develop technical competencies through hands-on experience, and progress employees into higher-level roles capable of independent analysis, incident response, and system optimization. This model

supports knowledge transfer, reduces reliance on external contractors, and ensures continuity of institutional knowledge critical to utility operations. Ultimately, these positions provide a scalable, utility-focused IT framework that aligns with industry best practices, enhances cybersecurity posture, and ensures GPA is equipped to meet both current and future operational demands.

B. *The essential details concerning the creation of the position. (see classification review below).*

C. *An analysis of similarities and differences between positions to be created and positions listed pursuant to 4 GCA, §4101.1(d);*

A review of existing comparable Government of Guam classifications, including Systems Analyst I & II, Systems Programmer, Systems Administrator, and the Guam Waterworks Authority (GWA) Network Analyst, reflects general similarities with the proposed positions in terms of core information technology functions such as network support, system maintenance, cybersecurity awareness, troubleshooting, and infrastructure monitoring. These roles all involve ensuring system reliability, supporting users, maintaining network connectivity, and safeguarding data and systems. For example, both Government of Guam and GWA classifications include responsibilities related to network performance monitoring, system optimization, and implementation of technology solutions to support organizational operations.

However, the proposed Information Security Analyst I & II and Network Systems Technician I & II classifications differ in that they are specifically designed to meet the operational demands of a public utility environment and incorporate a tiered I & II structure to support workforce development. Unlike existing classifications—which are often broader in scope or established at a fully qualified or higher-level entry point—the proposed positions provide a progressive framework that allows for entry-level recruitment, skill development, and advancement based on increasing complexity of work. This distinction is critical from a utility perspective, as it enables the Authority to build internal capacity, address recruitment challenges, and ensure continuity of operations through specialized, hands-on roles aligned with real-time system reliability and cybersecurity needs.

D. *The position description: See attached.*

E. *The proposed pay ranges and demonstration of compliance with §6301 of this Title; (see below) GPA's compensation plan was authorized by P.L. 28-159 and approved by the CCU in October 2007. The proposed compensation is in accordance with the Strategic Pay Plan Methodology.*

F. *A fiscal note as the term as described in 2 GCA, §9101 et seq.; and any other pertinent information.*

The Guam Power Authority is responsible for the funding availability for these positions and in compliance with all applicable laws, rules, and regulations regarding the creation, filling, and retention of positions in certified, technical, and professional positions. The funding of this position has no financial impact on the Government of Guam's General Fund.

2. The petition shall be posted on the agency, department, or public corporation's website for ten (10) days (Saturdays, Sundays, and government of Guam holidays excepted). After the posting, the head shall forward the petition along with evidence of his compliance with 4 GCA, Chapter 6, §6303.1(a), to the governing board or commission who, if they approve the same shall approve the petition by resolution and file the petition and resolution for records with the Director of Administration and the Legislative Secretary.

3. No new position may be filled until after compliance with the provision of this Section and thirty (30) days have elapsed from the date of filing with the Legislative Secretary.

III. METHODOLOGY

Information was gathered from various public utilities associated with the American Power Association (APPA) and other utilities with comparable positions within the U.S. mainland. The information collected was used to analyze and develop the proposed job standards as they apply to the work performed at GPA. The staff reviewed the duties associated with the proposed creations as indicated in the position descriptions. In evaluating these positions, the Strategic Pay Job Evaluation Methodology was utilized to determine the job evaluation points based on a total of twelve (12) measurement factors: Education, Experience, Complexity, Scope of Work, Problem Solving, Freedom to Act/Supervision Received, Work Environment, Physical Demands, Impact of Discretionary Decisions, Human Relations Skills/Contact, Authority Exercised, and Supervisor/Managerial Responsibility.

IV. RECOMMENDATION

1. To approve the creation of the Information Security Analyst I & II and Network Systems Technician I & II positions in the classified service and add the positions to the Certified, Technical, and Professional (CTP) list of positions.

2. To adopt proposed minimum and maximum range of compensation which is in accordance with the Authority's Strategic Pay Methodology, as follows:

Benchmark Position	40th Market Percentile (2022 Market data- 5 sub steps)									
	Structural Adjustment - MIN					Structural Adjustment - MAX				
	Base Salary	Hourly	Grade	Step	Sub Step	Base Salary	Hourly	Grade	Step	Sub Step
Information Security Analyst II	$ 73,395.49	$ 35.29	K	02	B	$ 76,375.64	$ 36.72	K	03	B
Information Security Analyst I	$ 66,026.10	$ 31.74	J	03	D	$ 68,707.02	$ 33.03	J	04	D
Network Systems Technician II	$ 70,088.03	$ 33.70	J	05	B	$ 72,933.89	$ 35.06	J	06	B
Network Systems Technician I	$ 62,460.00	$ 30.03	I	04	D	$ 64,997.09	$ 31.25	I	05	D

5/7/2026

JOSHUA D. MANIBUSAN
Personnel Specialist IV

5/7/2026

JON-REY P. AGUIGUI
Personnel Services Administrator

5/7/2026

BEATRICE P. LIMTIACO
Assistant General Manager, Administration

5/8/2026

JOHN M. BENAVENTE, P.E.
General Manager

INFORMATION SECURITY ANALYST I (GPA)

NATURE OF WORK:

This is routine professional work in supporting and analyzing the information security of networked computer systems and information assets.

Employees in this class assist in security monitoring, log review, and basic analysis to support the implementation, configuration, maintenance, and testing of cybersecurity tools, controls, and protective measures. Work includes performing routine security checks, validating backups, assisting with vulnerability assessments, and providing end-user support on security-related matters.

ILLUSTRATIVE EXAMPLES OF WORK: *(Any one position may not include all duties listed, nor do the examples cover all duties that may be performed.)*

Assists in collecting, organizing, and analyzing security log data to support threat monitoring, identify trends or anomalies, and prepare reports for management review and operational decision-making.

Provides support in the setup, configuration, and maintenance of endpoint devices, user accounts, passwords, multifactor authentication tools, and basic security controls under established procedures and supervision.

Troubleshoots routine security-related issues involving user access, antivirus alerts, endpoint protection systems, email security, and monitoring tools; performs preventative maintenance and coordinates escalations when necessary.

Performs routine verification of system, server, and database backups; assists in validating backup integrity, retention schedules, and compliance with established procedures for safeguarding backup media and recovery data.

Assists with the deployment of approved security patches, firmware updates, and software upgrades to systems, applications, and devices; coordinates with vendors or technical staff for product support, warranty issues, and service requests as necessary.

Supports cybersecurity personnel in evaluating, testing, and implementing security tools, software enhancements, configuration changes, and technology upgrades designed to strengthen the organization’s security posture.

Monitors and reviews system, server, and network activity to identify potential security concerns, suspicious behavior, or performance issues; analyzes basic trends and promptly escalates matters requiring advanced review.

Assists in administering security processes, including reviewing user access permissions, monitoring account activity, supporting password controls, and helping maintain the confidentiality, integrity, and availability of data across platforms.

Provides end-user support by responding to routine security inquiries, assisting with access requests, preparing documentation, and delivering basic training on secure computing practices, reporting procedures, and acceptable use requirements.

Assists with vulnerability scans, log reviews, and monitoring of security alerts to ensure compliance with established cybersecurity procedures.

Performs other related duties as required.

MINIMUM KNOWLEDGE, ABILITIES, AND SKILLS:

Knowledge of basic applicable principles, practices, methods, techniques, and tools used in cybersecurity monitoring, incident response, and security administration.

Knowledge of applicable basic principles of troubleshooting common security-related issues in computer systems, applications, and networks.

Ability to assist in configuring, monitoring, maintaining, and supporting cybersecurity tools, user access controls, endpoint security measures, and related protective technologies under supervision.

Ability to recognize, document, and promptly report potential vulnerabilities, security alerts, suspicious activity, or policy violations, and assist in applying standard corrective actions or mitigations.

Ability to perform routine troubleshooting of security-related problems, apply established solutions, and appropriately escalate more complex issues.

Ability to work collaboratively with colleagues, departments, and external partners in a professional and effective manner to support cybersecurity operations.

Ability to communicate effectively with users and staff while providing support for security awareness and safe computing practices.

Ability to understand and follow cybersecurity policies, procedures, oral instructions, and written guidelines.

MINIMUM EXPERIENCE AND TRAINING:

A) One (1) year of progressively responsible experience in information security and, network protection and maintenance, systems support, or cyber security-related work, and a Bachelor’s Degree in Computer Science, Computer Information Systems (CIS), Information Technology, Cybersecurity, or a closely related field; or

B) Any equivalent combination of experience and training that provides the required knowledge, abilities, and skills.

Established:

_____
Francis E. Santos, Chairman
Consolidated Commission on Utilities

INFORMATION SECURITY ANALYST II (GPA)

NATURE OF WORK:

This is moderately technical professional work in supporting information security of networked computer systems and information assets.

Employees in this class independently assignments with independence, including monitoring and evaluating security controls, investigating and troubleshooting complex security incidents, analyzing processes and data to identify risks and recommend improvements, and supporting the implementation of security tools, and protective measures. Employees are expected to exercise sound judgment, handle more complex assignments, and assist in training lower-level staff.

ILLUSTRATIVE EXAMPLES OF WORK: *(Any one position may not include all duties listed, nor do the examples cover all duties that may be performed.)*

Monitors, evaluates, and analyzes security events, logs, alerts, and system activity across servers, endpoints, applications, cloud environments, and network infrastructure; correlates data to identify suspicious activity, emerging threats, vulnerabilities, and operational risks; recommends corrective actions and supports secure, reliable operations across the organization.

Assesses and evaluates the security architecture of systems, applications, databases, servers, and network environments to ensure alignment with cybersecurity best practices, organizational policies, and applicable regulatory or compliance requirements; recommends enhancements to strengthen confidentiality, integrity, and availability of information assets.

Identifies, investigates, contains, and helps resolve complex cybersecurity incidents, unauthorized access attempts, malware infections, phishing events, data loss risks, and other security breaches; performs root cause analysis, documents findings, and serves as an escalation resource for threat detection, incident response, and recovery activities.

Monitors and verifies security-related backups, disaster recovery processes, and data integrity controls; develops and documents security procedures and recommends improvements to maintain operational continuity.

Performs advanced threat diagnostics, evaluates security tool performance, and coordinates with internal departments, contractors, and vendors to ensure implemented solutions meet security requirements, operational needs, and service expectations; reviews and validates completed work for quality and effectiveness.

Evaluates, selects, and recommends security tools, applications, and defensive technologies; leads implementation and testing of new security systems, upgrades, and integrations.

Monitors and optimizes security-related system and network performance, including intrusion detection, log retention, and endpoint protection.

Provides technical guidance, knowledge transfer, and on-the-job training to lower-level staff and users on cybersecurity awareness, secure practices, and proper use of information systems.

Implements and maintains protective measures by monitoring for vulnerabilities, applying critical security patches, managing endpoint defenses, and staying current with emerging cyber threats.

Performs other related duties as required.

MINIMUM KNOWLEDGE, ABILITIES, AND SKILLS

Knowledge of principles, industry practices, methods, techniques, tools, and technologies used in cybersecurity monitoring, incident response ad, security administration.

Knowledge of security monitoring tools, log management systems, vulnerability management processes, incident response procedures, backup and recovery practices, and access control methods.

Knowledge of current and emerging cyber threats, attack techniques, defensive technologies, and industry best practices.

Knowledge of applicable laws, regulations, compliance standards, and organizational policies governing information security and data protection.

Ability to investigate, troubleshoot, and resolve security incidents, system vulnerabilities, and access control issues; assess systems and processes to identify deficiencies and recommend corrective improvements; and configure, maintain, and evaluate cybersecurity tools, backup, recovery, and continuity measures to ensure operational resilience and data integrity.

Ability to prepare clear and concise reports, technical documentation, procedures, and recommendations.

Ability to communicate effectively, both orally and in writing, with technical personnel, management, vendors, and end users.

Ability to provide guidance to lower-level staff and users regarding secure practices and cybersecurity awareness.

MINIMUM EXPERIENCE AND TRAINING:

A) Two (2) years of progressively responsible experience in in information security and, network protection and maintenance, systems support, or cyber security-related work,

and a a Bachelor's Degree in Computer Science, Computer Information Systems (CIS), Information Technology, Cybersecurity, or a closely related field; or

B) Any equivalent combination of experience and training that provides the required knowledge, abilities, and skills;

Established:

_____

Francis E. Santos, Chairman
Consolidated Commission on Utilities

NETWORK SYSTEMS TECHNICIAN I (GPA)

NATURE OF WORK:

This is semi-skilled technical work involving the support, maintenance, and analysis of networked computer systems, communications equipment, and related technology infrastructure.

Employees in this class assist with system monitoring, data collection, and technical analysis to support the installation, configuration, maintenance, and testing of computer hardware, software, servers and other network system devices. Employees work under supervision while learning established technical procedures, developing diagnostic skills, and gaining proficiency for more complex assignments.

ILLUSTRATIVE EXAMPLES OF WORK: *(Any one position may not include all duties listed, nor do the examples cover all duties that may be performed.)*

Assists in collecting, organizing, and reviewing system and network data to support performance monitoring, identify trends, and prepare reports for operational review and decision-making.

Provides support in setting up, installing, and configuring desktop computers, laptops, printers, telephones, mobile devices, servers, and network connections, including basic cabling, wiring, and peripheral equipment.

Assists with the installation, relocation, and testing of network hardware such as routers, switches, wireless access points, modems, and related communications equipment under established procedures and supervision.

Troubleshoots routine hardware, software, connectivity, and user access issues; performs preventative maintenance and coordinates escalations for more complex technical problems when necessary.

Performs routine system, server, and database backups; assists in verifying backup completion and follows established procedures for storing, safeguarding, and rotating backup media.

Conducts minor repairs and replacements on computer systems, printers, phones, scanners, and related devices; coordinates with vendors or service providers for warranty claims, parts, or on-site support as required.

Assists information technology staff in evaluating, testing, and implementing hardware upgrades, software updates, patches, and other system enhancements designed to improve performance and reliability.

Monitors computer systems, networks, and applications to identify outages, errors, capacity concerns, or performance issues; documents findings, analyzes basic trends, and escalates concerns as appropriate.
Provides end-user technical support by responding to service requests, assisting with passwords and account access, preparing documentation, and delivering basic training on system functions, reporting tools, and access procedures.

Keeps current with information technology trends, hardware developments, and technical procedures through assigned training, manuals, and professional reading.

Performs other related duties as required.

MINIMUM KNOWLEDGE, ABILITIES, AND SKILLS:

Knowledge of the basic principles, practices, methods, techniques, tools, and test equipment used in the installation, maintenance, repair, and support of network infrastructure, computer systems, and related equipment.

Knowledge of standard troubleshooting methods used to diagnose hardware, software, printer, communication, and network connectivity problems.

Knowledge of basic cybersecurity concepts, including password security, antivirus protection, user access controls, and safe computing practices.

Ability to analyze, install, configure, and maintain the operations of network systems, servers, desktop computers, and peripheral devices.

Ability to analyze and troubleshoot complex computer system and network issues, identify the reasons for network and network device problems, failures and malfunctions and apply established solutions while appropriately escalating more complex matters.

Ability to use diagnostic tools, testing devices, manuals, and technical documentation in the performance of assigned work.

Ability to work collaboratively with colleagues, departments, and the public in a professional and effective manner.

Ability to understand and follow oral and written instructions.

MINIMUM EXPERIENCE AND TRAINING:

A) Two (2) years of experience in network operating systems, server administration, system maintenance, troubleshooting, or related information technology work; or

B) Any equivalent combination of experience and training that provides the required knowledge, abilities, and skills.

Established:

_____
Francis E. Santos, Chairman
Consolidated Commission on Utilities

NETWORK SYSTEMS TECHNICIAN II (GPA)

NATURE OF WORK:

This is moderately technical work involving the support, analysis, monitoring, and administration of networked computer systems, communications equipment, and related technology infrastructure.

Employees in this class perform assignments with independence and are responsible for evaluating system and network performance, troubleshooting more complex hardware, software, server, and connectivity issues, and analyzing data to recommend operational improvements. Work includes implementing, configuring, maintaining, and testing system upgrades, network improvements, and security controls. Responsibilities may also include coordinating with vendors, evaluating and integrating new technologies, and providing technical guidance and training to lower-level staff.

ILLUSTRATIVE EXAMPLES OF WORK: *(Any one position may not include all duties listed, nor do the examples cover all duties that may be performed.)*

Independently monitors, evaluates, and analyzes the performance, availability, and reliability of computer systems, servers, telecommunications equipment, and network infrastructure; uses data and trend analysis to identify issues, recommend improvements, and support efficient network operations across the organization.

Analyzes, plans, and evaluates network and system infrastructure, including computers, phones, servers, switches, routers, and cabling layouts, ensuring compliance with ensures configurations meet operational requirements, industry standards, and organizational policies.

Identifies, investigates, troubleshoots, and resolves complex hardware, software, server, communications, and network connectivity problems; performs root cause analysis and serves as a technical resource for escalated issues.

Monitors and verifies system and database backups, develops and documents procedures, and recommends improvements to maintain data integrity and operational continuity.

Performs technical diagnostics using network monitoring tools, test equipment, and system utilities; evaluates system health, performance, and capacity, and coordinates corrective actions to maintain service levels.

Evaluates, selects, recommends, and assists in implementing hardware, software, server, and network enhancements; leads or coordinates testing of new systems, upgrades, migrations, and technology integrations.

Monitors and optimizes system and network performance, including response times, storage capacity, bandwidth utilization, and overall resource allocation.

Performs higher-level network administration duties such as configuring applications, managing security permissions, creating and modifying access control policy, and maintaining network documentation.

Provides advanced technical support to users and departments regarding hardware, software, connectivity, and enterprise applications; develops user guides, training materials, and conducts instruction on system functions, productivity tools, and safe computing practices.

Participates in technology projects by contributing expertise, preparing cost estimates, and coordinating with other departments to ensure smooth implementation.

Researches and evaluates new technologies, tools, and industry practices to improve system performance, operational efficiency, communications reliability, and cybersecurity readiness; identifies opportunities for modernization and innovation.

May provide guidance or training to lower-level technicians in troubleshooting, best practices, and technical procedures.

Performs other related duties as required.

MINIMUM KNOWLEDGE, ABILITIES, AND SKILLS

Knowledge of the basic principles, practices, methods, techniques, tools, and test equipment used in the installation, maintenance, repair, and support of network infrastructure, computer systems, and related equipment.

Knowledge of advanced troubleshooting methods used to diagnose hardware, software, printer, communication, and network connectivity problems.

Knowledge of cybersecurity fundamentals, including access controls, patch management, endpoint protection, password security, and safe computing practices.

Ability to independently install, configure, maintain, administer, and monitor network systems, servers, desktop computers, printers, telephones, and related peripheral equipment to ensure reliable operations.

Ability to analyze and resolve complex computer system and network issues by determining root causes of device failures, connectivity problems, software malfunctions, or performance limitations, and developing effective technical solutions.

Ability to serve as a technical resource to other staff by providing guidance in troubleshooting, systems optimization, network administration, and established technical procedures.

Ability to prepare clear, concise, and accurate reports, technical documentation, inventories, diagrams, procedures, and other written materials.
Ability to work collaboratively with colleagues, departments, and the public in a professional and effective manner.

Ability to understand, interpret, and apply oral and written instructions independently, exercising sound judgment in decision-making.

MINIMUM EXPERIENCE AND TRAINING:

A) Two (2) years of progressively responsible experience in network operating systems, server administration, system maintenance, troubleshooting, or related information technology work and graduation with a Bachelor's degree from a recognized college or university in Computer Science, Computer Information Systems (CIS), Information Technology or related field; or

B) Any equivalent combination of experience and training that provides the required knowledge, abilities, and skills.

Established:

_____
Francis E. Santos, Chairman
Consolidated Commission on Utilities