Judiciary of Guam

Administrative Office of the Courts
Guam Judicial Center • 120 West O'Brien Dr • Hagåtña, Gu. 96910
Tel: (671) 475-3544 • Fax: (671) 475-3184

Hon. Robert J. Torres
Chief Justice

Hon. Alberto C. Lamorena, III
Presiding Judge

Danielle T. Rosete, Esq.
Administrator of the Courts

May 29, 2025

MEMORANDUM:

To: All Prospective Offerors

From: Administrator of the Courts

Subject: **Amendment No. 8**
Re: RFP 25-06; Upgrade of Access Control System and Provide and Install CCTV

Below are responses to questions submitted to my office.

1. Kindly confirm if detailed documentation, including schematics of the existing Access Control System (ACS), hardware inventory, software versions, and network infrastructure, will be provided to facilitate accurate assessment and planning.
   Response:
   - **Unfortunately, there are no schematics for the existing ACS and network infrastructure.**
   - **To be replaced: previous Software versions - RISG Administrator version 5.4.1.0 & RISG Alarms version 7.6.0.2**
   - **Hardware Inventory: Please see Question 2.**

2. Please specify the current brands and models of access control components deployed (e.g., panels, readers, controllers, biometric devices) to determine compatibility with proposed solutions.
   Response:
   - **Proximity Cards: HID 0008P 11101004444-1, Starting at 301**
   - **HID Card Readers (29): Unknown Model, See Attachment 1 for placement**
   - **REX Devices: Each RFID door is paired with a REX device (24)**
   - **RCI 4114-05 Electric Strikes: Twenty-three (23) RFID doors**
   - **Seco-Larm 600lb Magnetic Lock, E-941SA-600: One side of the double-glass door. NOTE: A second magnetic lock is needed**

- **Aiphone Control with intercom, video, and access control of double door and gate (1): Controlled the double-glass door and the rolling gate.**
- **Gate Latches (2): Unknown Model. These will need replacement due to severe corrosion.**
- **Door access controller panels: 8-door & 4-door**
- **Gate Operator: Model - Lift Master Elite Series; Motor YSLB-250-4-B001, 1/2 HP, Type F, up to 1000 lbs.**

3. For the requested keypad entry option, please clarify the number and locations of doors where dual authentication (keypad and proximity reader) is anticipated.
Response:
Three (3) doors will require keypad/pin entry and proximity card readers.
    - **Firing Range**
    - **Drug Evidence**
    - **Drug Standards**

4. Can existing cabling infrastructure be utilized, or should Offerors assume that new pathways and wiring installations will be necessary throughout the facility?
Response:

    - **Yes, existing cabling infrastructure can be utilized where possible. The CCTV and the keypad/pin entry are new installations and may require additional/new wiring.**

5. Is continuous system operation required during the upgrade, or will there be scheduled downtime windows permissible for transition activities?
Response:

    - **Scheduled downtime windows are allowed for transition activities. However, at the end of each business day, the laboratory and designated areas must be secured in accordance with the applicable protocols.**

6. Are there defined requirements regarding system redundancy, failover capabilities, and disaster recovery protocols?
Response:

    - **System Redundancy: Critical hardware components (servers, network infrastructure, power supplies) shall have redundant configurations to avoid single points of failure and ensure uninterrupted operation. Data storage must employ RAID or equivalent technologies to safeguard against disk failures. Network redundancy shall maintain connectivity during component outages. All redundant elements must enforce strict security protocols to**

protect forensic data and preserve chain of custody.

- **Failover Capabilities: The system shall support automatic failover within 60 seconds or less, ensuring minimal downtime. Failover must maintain data integrity, audit trails, and system logs. Regular failover testing and documentation are required. Failover events must be logged comprehensively for audit purposes.**
- **Disaster Recovery Protocols: Scheduled secure backups of all critical data and system configurations shall be performed (e.g., daily incremental, weekly full backups). Backup data must be encrypted in transit and at rest. A formal Disaster Recovery Plan (DRP) must define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) tailored for forensic operations, and outline procedures for restoring system functionality after failures or disasters. Annual DR drills are recommended to ensure effectiveness and preparedness. Detailed logs of backup, recovery, and failover activities shall be maintained for chain-of-custody and audit compliance.**

7. For remote access functionalities, please advise if there are mandated cybersecurity measures such as VPN configurations or firewall policies to be implemented.
Response:

- Yes, remote access functionalities must adhere to strict **cybersecurity and compliance standards**, including **CJIS (Criminal Justice Information Services) compliance**. These standards require that any access to criminal justice systems, including CCTV systems used for law enforcement purposes, be secured through encrypted and authenticated channels.

  This function is best handled by the **Office of Technology (OTECH)**, which manages the **SonicWall firewall and VPN infrastructure** for the Government of Guam. All remote access to the CCTV system must be routed through OTECH's **SonicWall VPN**, and OTECH will be responsible for:

  - Configuring and managing secure **VPN access**
  - Implementing and updating **firewall rules** to control incoming/outgoing traffic

- Ensuring all connections are **encrypted (e.g., AES-256)** and **authenticated**
- Maintaining **access logs and audit trails** as required under CJIS
- Restricting access to **authorized personnel only**

Coordination with OTECH is required as part of the **scope of work** to ensure all configurations meet local government and **federal cybersecurity standards**, including CJIS, TAA, and NDAA compliance.

8. Will the Judiciary provide network resources (e.g., IP addresses, VLAN configurations), or is the Offeror expected to provision a dedicated network segment for the ACS?
Response:

- If needed, coordination through OTECH for the **network resources** necessary to support the ACS (Access Control System), including **IP address assignments, VLAN configurations, and network segmentation** must be made. This ensures integration with the existing infrastructure and compliance with internal security and access control policies.

  However, the **Offeror is expected to coordinate closely with the GPD's IT team** and/or OTECH to ensure proper configuration and compatibility. If a **dedicated network segment** is required for the ACS for performance or security reasons, the Offeror must clearly specify this in their scope of work, and GPD/OTECH will evaluate and provision resources accordingly.

  All network configurations must align with **CJIS, federal cybersecurity policies, and GPD-specific requirements**.

9. We kindly request confirmation on the total number of cameras anticipated for both indoor and outdoor coverage, and whether a facility layout or site plan will be provided to guide optimal placement.

Response:

- We anticipate a total of **14 cameras** for comprehensive coverage. This may be subject to change if other considerations arise during the onsite inspection or if adjustments are deemed necessary to address unforeseen security or operational needs.
  - **8 interior cameras** – to monitor hallways, entry points, common areas, and sensitive workspaces

- **6 exterior cameras** – to cover building entrances, parking areas, perimeter zones, and any vulnerable access points

Yes, a **facility layout or site plan will be provided** to guide optimal camera placement. This layout will assist in identifying key coverage areas, eliminating blind spots, and ensuring proper field-of-view overlap for enhanced security. Final camera placement will be confirmed during a walk-through with relevant stakeholders.

10. Please clarify the availability and capacity of the existing network infrastructure, including PoE switches and bandwidth, for supporting CCTV connectivity.

Response:

- The availability and capacity of the **existing network infrastructure** to support CCTV connectivity are currently under assessment. Preliminary observations indicate that:
  - **PoE Switches:** Limited existing PoE switch capacity is available. However, depending on final camera counts and placement, **additional PoE switches** may be required to support power and data transmission for all IP cameras.
  - **Bandwidth:** The current network has sufficient internal bandwidth for standard office operations. However, **dedicated bandwidth may be needed** for CCTV traffic to ensure uninterrupted video streaming and recording, particularly if using high-resolution (4MP or higher) cameras.
  - **Segmentation:** It is recommended that CCTV devices be placed on a **dedicated VLAN** to isolate video traffic and enhance performance and security.

A full infrastructure evaluation will be conducted in collaboration with the Judiciary's or GPD's IT team to determine if **upgrades to switches, cabling, or bandwidth provisioning** will be necessary.

11. Is there an existing Video Management System (VMS) in place, or should a new VMS platform be included within the proposal?

Response:

- **There is <u>no</u> existing VMS. Please include a new VMS platform within the proposal.**

12. Beyond the stated 30-day storage requirement, are there additional specifications concerning video resolution, frame rates, or data retention policies?

Response:

- **Video Resolution: The system should support a minimum resolution of 1080p (Full HD) to ensure clear and detailed video suitable for forensic review. Higher resolutions may be necessary for critical areas.**

- **Frame Rate: A minimum frame rate of 15 to 30 frames per second (fps) to provide smooth motion capture while optimizing storage use. Higher frame rates may be applied in specific zones requiring enhanced detail.**

- **Data Retention: In addition to the baseline 30-day video retention requirement, the system should support configurable data retention periods to align with operational needs and forensic protocols. This includes the ability to:**

  - **Adjust retention periods for different camera zones or event types (e.g., general monitoring vs. evidence-handling areas).**

  - **Extend retention for footage associated with incidents, investigations, or internal audits, up to 90 days or longer as required.**

  - **Flag and archive specific video segments indefinitely for case-related purposes, ensuring they are securely stored, access-controlled, and retrievable on demand.**

  - **Apply retention rules based on administrative policy or user-defined tags, allowing for flexible and policy-driven video lifecycle management.**

  - **The system should provide secure administrative controls to manage retention schedules and ensure compliance with organizational and operational requirements.**

13. For outdoor camera installations, are there designated areas where solar-powered solutions are mandatory due to limited access to electrical infrastructure?

Response:

- At this time, there are **no designated areas where solar-powered camera solutions are mandatory**. However, during the site inspection, several exterior locations were identified as having **limited or no direct access to electrical infrastructure**. For these specific locations, **solar-powered surveillance solutions with battery backup** may be considered as an alternative to trenching or electrical conduit installation.

  If solar power is to be implemented, the following must be considered:

  - **Sunlight exposure and panel positioning**
  - **Battery capacity and autonomy for overnight and low-sunlight days**
  - **Wireless data transmission options (e.g., point-to-point Wi-Fi or LTE)**
  - **Weatherproof and vandal-resistant enclosures**

  A final determination will be made based on **site conditions, feasibility assessments, and power infrastructure evaluations** conducted in coordination with relevant personnel.

14. Are advanced video analytics features (e.g., motion detection, intrusion alerts, license plate recognition) required for this deployment?

Response:

- Yes, **advanced video analytics features** are **recommended** for this deployment to enhance situational awareness and support investigative capabilities. The following features should be considered as part of the system design:
  - **Motion Detection:** To trigger recording and alerts in areas with low traffic or during off-hours
  - **Intrusion Alerts:** To notify security personnel of unauthorized access to restricted areas or after-hours movement
  - **License Plate Recognition (LPR):** Recommended for exterior cameras covering parking lots or vehicle entry/exit points, particularly in areas with controlled access

- **Tamper Detection:** To alert if a camera is obscured, moved, or otherwise disabled

- **People Counting / Object Tracking (Optional):** Useful in monitoring occupancy or suspicious behavior in sensitive areas

These features must be compatible with **CJIS-compliant systems** and should integrate with the **NVR or VMS (Video Management System)** being proposed.

Final analytics requirements will be determined based on operational needs, available budget, and stakeholder input.

15. Is integration between the CCTV and Access Control Systems required, such as event-based video recording triggered by access events?

Response:

- **Yes, if CCTV is included in the final proposal, integration between the CCTV and Access Control Systems (ACS) is strongly recommended to enhance security monitoring and incident response. This integration is essential for maintaining synchronized audit trails, enhancing security monitoring, and ensuring compliance with applicable laboratory accreditation and operational standards. It should support the following key features:**

  - **Event-Based Video Recording: The CCTV system should be capable of automatically recording video clips triggered by access control events, such as door openings, denied access attempts, after-hours entries, or forced entries.**

  - **Real-Time Notifications: Security personnel should receive real-time alerts with associated video when specific access events occur.**

  - **Time-Stamped Synchronization: Access control logs and video footage should be time-synchronized to allow seamless review of events.**

  - **Unified Interface (Optional): If possible, integration into a single monitoring platform or dashboard for both systems is preferred to streamline operations.**

- **Compliance: The integrated solution must comply with CJIS, NDAA, and Judiciary IT policies.**

Integration will be coordinated with the ACS provider and network team to ensure compatibility and secure communication between systems.

16. Are there specific cybersecurity standards applicable to IoT devices within this project scope, particularly for networked CCTV systems?

Response:

- Yes, specific **cybersecurity standards** apply to all **IoT devices** within the project scope, particularly for **networked CCTV systems**. These systems must adhere to the following applicable standards to ensure security, data integrity, and compliance with both federal and local policies:

1. CJIS Security Policy

- All network-connected devices (including CCTV and access control systems) must comply with the **FBI CJIS Security Policy**, particularly regarding encryption, authentication, audit logging, and access control.

2. NDAA Section 889 Compliance

- CCTV equipment must be **NDAA-compliant**, meaning it **cannot include components from banned manufacturers** such as Hikvision, Dahua, and Huawei. This is a federal procurement requirement.

3. TAA Compliance

- For federal funding or contract eligibility, devices should be **TAA-compliant** (Trade Agreements Act), ensuring that components are manufactured or substantially transformed in designated countries.

4. Network Security Best Practices

- Devices must support:
  - **AES-256 encryption** for data in transit

- **HTTPS and SSL/TLS** secure communication protocols
- **Role-based access control**
- **Firmware validation and secure boot processes**
- **Automatic security patching or update mechanisms**

5. Local Policy (OTECH / GovGuam)

- All IoT and CCTV devices must be reviewed and approved in accordance with **OTECH network security policies**, including firewall rules, VLAN segmentation, and **SonicWall VPN use** for remote access.

17. Please specify the required Camera Resolution required for both indoor and outdoor cameras.

Response:

- **The following minimum camera resolution requirements are specified to ensure adequate image clarity for identification and investigative purposes:**

Indoor Cameras:

- **Minimum Resolution: 4MP (2560 x 1440)**
- **Purpose: General surveillance of hallways, entryways, offices, and common areas**
- **Features: Wide Dynamic Range (WDR), low-light performance (at least 0.01 lux), and IR illumination preferred**

Outdoor Cameras

- **Minimum Resolution: 4MP to 8MP (3840 x 2160 for UHD)**
- **Purpose: High-definition monitoring of building perimeters, parking lots, and vehicle entry/exit points**
- **Features: IP66/67 weatherproof housing, IR/night vision, vandal resistance (IK10), and Wide Dynamic Range (WDR) for handling varied lighting conditions**

All cameras must support ONVIF compliance, be NDAA compliant, and integrate seamlessly with the proposed VMS/NVR solution. Higher resolutions may be proposed for specific use cases such as License Plate Recognition (LPR) or facial identification zones.

The deadline to submit proposals is changed from **June 3, 2025 at 10am, Guam Standard Time, to June 9, 2025 at 2pm, Guam Standard Time.**

Please be reminded that this Amendment shall be acknowledged in your proposals. Failure to acknowledge this Amendment No. 8 may result in disqualification from this RFP.

Should you have any questions please contact the Procurement office at **(671) 300-7994/475-3212/3175** or email at mantonio@guamcourts.gov and kperez@guamcourts.gov.

DTRosete
DANIELLE T. ROSETE

cc: RFP File