DRAFT PERFORMANCE WORK STATEMENT (PWS)

Modernized Electronic Security System

Fort Norfolk, Norfolk, Virginia

Draft for Pre- Solicitation

Document Control Note:

This draft PWS is prepared for Pre- Solicitation purposes. It is not a solicitation, request for quotation, request for proposal, invitation for bid, or commitment by the Government. The final solicitation and resulting contract may revise, add, remove, or clarify any requirement after completion of acquisition planning, market research, legal review, security review, cybersecurity review, technical review, and Contracting Officer approval.

Public Posting Note:

This draft intentionally avoids disclosing detailed security vulnerabilities, final system layouts, camera views, detailed access-control configurations, internal network architecture, or other sensitive facility information. Any additional details required for proposal preparation should be released only after appropriate review and in accordance with the final acquisition strategy and public-release requirements.

PART 1 - GENERAL INFORMATION

1.1 General

This is a non-personal services requirement. Contractor personnel performing under the resulting contract shall not be subject, either by contract terms or by the manner of contract administration, to the supervision and control normally prevailing in relationships between the Government and its employees. The Contractor shall be responsible for managing, supervising, and directing its employees and subcontractors in performance of the work.

1.2 Description of Services

The Contractor shall provide non-personal services. The Contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, management, software, licensing, testing instruments, documentation, and other items necessary to furnish, install, integrate, test, commission, document, train, and maintain a modernized Electronic Security System (ESS) at Fort Norfolk, Virginia. The Contractor shall perform the work in accordance with the standards, acceptable quality levels, performance requirements, and associated contract documents identified in this Performance Work Statement.

The requirement includes modernization of Fort Norfolk's physical and electronic security posture through delivery of a complete and operational access control, video surveillance, security monitoring, perimeter gate, and perimeter fencing solution. The Contractor shall provide a fully functional physical access control management system compatible with the existing security environment currently using "AMAG Symmetry," or a functionally equivalent/interoperable solution that meets the Government's operational requirements as identified in the final solicitation. The system shall include required servers, workstations, software, licensing, system components, credential management capability, user permissions, audit capability, badging functionality, and centralized administration.

The Contractor shall replace or upgrade required access control devices, including access card readers and credential readers compatible with existing credentialing requirements, including "HID-compatible readers," at designated controlled entry points, doors, turnstiles, and gates. The Contractor shall also provide handheld credential verification and badge scanner devices functionally equivalent to "Telaeris XPID201" where required by the final solicitation and approved design.

The Contractor shall provide a complete video surveillance system and video management software platform capable of integrating with, or providing functionality comparable to, the existing environment currently using

"Milestone Professional+." The video surveillance solution shall support real-time monitoring, recording, playback, user access control, camera management, video retention, centralized viewing, and Government-designated monitoring functions. The system shall include cameras, recording and storage capability, monitoring workstations, displays, software licensing, cabling, mounting hardware, networked components, and all supporting equipment necessary for a complete, usable, and maintainable system.

The Contractor shall integrate the access control system, video surveillance system, security monitoring capability, gate controls, and related electronic security components into a complete, compatible, tested, and operational security system. The completed system shall allow designated Government personnel to manage access permissions, monitor entry control points, view and record video surveillance, support entry-control and guard-force operations, and support response to unauthorized access or security events.

The Contractor shall replace and upgrade designated perimeter fencing, vehicle gates, pedestrian gates, gate operators, controls, safety devices, sensors, and remote operating devices necessary to support Fort Norfolk's access control and perimeter security requirements. Fence and gate work shall be performed in accordance with approved submittals, manufacturer requirements, applicable Unified Facilities Criteria, installation security requirements, and the final contract documents.

The Contractor shall provide all required project management, quality control, safety management, installation coordination, submittals, shop drawings, testing plans, system configuration, functional testing, commissioning, troubleshooting, deficiency correction, training, warranties, operations and maintenance manuals, as-built documentation, and closeout materials. Final acceptance shall occur only after the system is fully installed, integrated, tested, documented, free of critical deficiencies, and accepted by the Government.

1.3 Background

Fort Norfolk requires modernization of its physical and electronic security posture to protect personnel, facilities, and Government resources. The Government anticipates that a modernized ESS will improve access-control operations, video surveillance capability, security monitoring, perimeter security, and maintainability of the overall security environment. This draft PWS is provided for market research so industry can identify its ability to provide compatible, interoperable, or functionally equivalent solutions that meet the Government's operational needs.

1.4 Scope

The Contractor shall design, furnish, install, integrate, test, commission, document, train, and maintain a fully operational ESS and related perimeter fence/gate improvements at Fort Norfolk. The scope includes project management, site coordination, submittals, access control, video surveillance, system integration, gate and fence improvements, quality control, safety, testing, training, warranty support, and closeout documentation. Specific quantities, locations, configurations, and sensitive details will be established in the final solicitation and approved design documents.

1.5 Objectives

- Modernize and improve Fort Norfolk access-control capability.
- Modernize and improve video surveillance and monitoring capability.
- Provide a complete, integrated, and maintainable electronic security solution.
- Improve designated perimeter fencing, gates, operators, controls, and related access infrastructure.
- Deliver a system that is installed, integrated, tested, commissioned, documented, and ready for Government acceptance.
- Support Government security operations without disclosing sensitive facility vulnerabilities in public acquisition documents.

1.6 Acquisition and Contract Type Alignment

This requirement may include a combination of supply, service, installation, integration, testing, commissioning, training, and construction-type site work. The final acquisition method, contract type, clauses, wage determination

requirements, construction-related provisions, cybersecurity requirements, brand-name or brand-name-or-equal approach, and small-business strategy will be determined by the Contracting Officer after completion of acquisition planning and market research.

1.7 Brand-Name / Existing Environment References

Any brand-name references in this draft PWS are provided for market research purposes to describe the existing environment, anticipated compatibility needs, or functional capability currently understood by the Government. Brand-name references do not, by themselves, establish the final solicitation approach. The final solicitation may identify brand-name, brand-name-or-equal, compatibility, interoperability, or functionally equivalent requirements after appropriate review, documentation, and Contracting Officer approval.

Generic Functional Description	Existing Environment / Brand Reference	Draft Market Research Treatment
Physical access control management system	"AMAG Symmetry"	Identify firms capable of providing a compatible, interoperable, or functionally equivalent solution that meets Government operational requirements.
Access card readers / credential readers	"HID-compatible readers"	Identify credential reader compatibility and access-control integration capability.
Handheld credential verification / badge scanner devices	"Telaeris XPID201"	Identify devices capable of equivalent badge/credential verification functionality and integration.
Video surveillance system / video management software platform	"Milestone Professional+"	Identify firms capable of providing compatible, interoperable, or comparable VMS functionality.

1.8 Quality Control Plan

The Contractor shall develop, submit, implement, and maintain a Quality Control Plan (QCP) to ensure contract performance complies with the PWS, approved submittals, manufacturer requirements, safety requirements, and resulting contract. The Contractor shall submit the proposed QCP to the Contracting Officer through the COR within 10 calendar days after contract award, unless otherwise stated in the final solicitation.

- Organizational structure and key responsibilities.
- Inspection procedures and acceptance checks.
- Submittal, configuration, and deliverable control procedures.
- Testing procedures and deficiency tracking.
- Corrective action procedures and recurrence prevention.
- Installation access control and personnel accountability procedures.
- Documentation retention and turnover procedures.

1.9 Quality Assurance

The Government will evaluate Contractor performance in accordance with the Quality Assurance Surveillance Plan (QASP), the Performance Requirements Summary (PRS), approved submittals, and the resulting contract. Government surveillance may include inspection, document review, functional testing, acceptance testing, meeting participation, deficiency review, and verification of corrective actions.

1.10 Place of Performance

Work will be performed at Fort Norfolk and associated Government-designated facilities located at or near 803 Front Street, Norfolk, Virginia. The Government will identify exact work areas, access limitations, and site coordination requirements in the final solicitation and during performance.

1.11 Work Hours and Site Coordination

Unless otherwise approved by the Contracting Officer, on-site work shall be performed during normal installation operating hours, Monday through Friday, excluding federally recognized holidays. Work outside normal hours shall be coordinated in advance and shall not proceed unless approved by the Contracting Officer or authorized

Government representative. The Contractor shall coordinate work to minimize disruption to Government operations and maintain safe access to occupied facilities.

1.12 Security, Access, Information Protection, and Cybersecurity

The Contractor shall comply with all installation access, physical security, information protection, cybersecurity, antiterrorism, operations security, badging, training, and security-related requirements identified in the final solicitation and resulting contract. The Government will complete applicable security review documentation as part of the requirements package and will incorporate any required security provisions, clauses, training requirements, or access-control requirements into the solicitation and contract.

Contractor personnel shall not begin work requiring access to Government facilities, Government systems, Government information, or security-sensitive areas until all applicable access, screening, training, and badging requirements have been satisfied. The Contractor shall safeguard Government information, Government property, and security-sensitive information encountered during performance. Any Federal Contract Information (FCI), Controlled Unclassified Information (CUI), cybersecurity, or CMMC-related requirements shall be determined during acquisition planning and incorporated into the final solicitation and resulting contract if applicable.

The Contractor shall not connect equipment to Government enterprise networks unless expressly authorized in writing by the Government and in accordance with the final contract requirements. Where standalone, isolated, or logically separated network operation is required, the Contractor shall provide the necessary components, configuration, hardening, and documentation required by the final solicitation and approved design.

1.13 Key Personnel

The Contractor shall designate an on-site project manager or superintendent and an alternate in writing to the COR. The designated representative shall be responsible for day-to-day coordination, schedule management, subcontractor coordination, submittal management, testing support, deficiency correction, training coordination, and closeout support until final Government acceptance.

1.14 Meetings

The Contractor shall attend a post-award conference, progress meetings, coordination meetings, testing meetings, and acceptance meetings as requested by the Government. Meetings may be conducted in person or virtually at the Government's discretion. Meeting attendance shall be included in the contract price unless otherwise stated in the final solicitation.

1.15 Safety

The Contractor shall comply with applicable Federal, state, local, installation, OSHA, and U.S. Army Corps of Engineers safety requirements incorporated into the contract. Before physical work begins, the Contractor shall submit required safety documentation, including an Accident Prevention Plan and applicable Activity Hazard Analyses, for Government review and acceptance when required by the final solicitation.

1.16 Training

Contractor personnel shall complete and document all training required by the final solicitation and resulting contract for installation access, facility security, antiterrorism, operations security, cybersecurity, safety, and performance of the work. Training certificates or records shall be provided to the COR when required by the contract.

1.17 Data Rights, Non-Disclosure, and Organizational Conflict of Interest

All documents, drawings, submittals, system configurations, data, and deliverables produced under the resulting contract shall be subject to the rights, non-disclosure, and organizational conflict of interest requirements incorporated into the final solicitation and resulting contract. The Contractor shall not release Government information or security-sensitive information without Government authorization.

PART 2 - DEFINITIONS AND ACRONYMS

Term	Meaning

Term	Meaning
ACS	Access Control System.
ATO	Antiterrorism Officer, when applicable to Government security review processes.
CCTV	Closed-Circuit Television; commonly used as a general reference to video surveillance.
COR	Contracting Officer's Representative.
CUI	Controlled Unclassified Information, if applicable to the final requirement.
ESS	Electronic Security System.
FCI	Federal Contract Information, if applicable to the final requirement.
KO	Contracting Officer.
O&M	Operations and Maintenance.
OPSEC	Operations Security.
PRS	Performance Requirements Summary.
QASP	Quality Assurance Surveillance Plan.
QCP	Quality Control Plan.
VMS	Video Management Software/System.
VSS	Video Surveillance System.

PART 3 - GOVERNMENT-FURNISHED PROPERTY, INFORMATION, AND ACCESS

The Government will provide access to the site as necessary for performance and will identify Government points of contact for coordination. The Government may provide existing system information, facility access requirements, site-specific constraints, and other Government-furnished information after appropriate review and in accordance with the final solicitation and contract. The Contractor shall protect all Government-furnished information and shall return or dispose of such information as directed by the Government.

No Government-furnished property is anticipated unless specifically identified in the final solicitation or resulting contract. The Contractor shall not rely on access to Government equipment, tools, storage areas, network infrastructure, or facilities unless expressly authorized in writing.

PART 4 - CONTRACTOR-FURNISHED ITEMS AND SERVICES

The Contractor shall furnish all labor, supervision, management, materials, components, devices, software, licensing, tools, equipment, transportation, testing instruments, temporary facilities, documentation, training materials, and other resources necessary to complete the work described in this PWS unless expressly identified as Government-furnished property or information in the final solicitation.

PART 5 - SPECIFIC TASKS

5.1 Project Management, Planning, and Coordination

The Contractor shall manage the work from award through final acceptance. The Contractor shall coordinate work with the COR, Government security personnel, facility personnel, and other Government representatives as directed. The Contractor shall submit and maintain a project schedule identifying major tasks, submittals, site work, installation phases, testing events, training, deficiency correction, and closeout activities.

- Attend post-award, progress, coordination, testing, and closeout meetings as required.
- Maintain an updated project schedule and identify critical path activities.
- Coordinate site access and installation activities in advance.
- Track submittals, deficiencies, corrective actions, and closeout items.
- Protect Government operations and avoid unnecessary disruption to occupied facilities.

5.2 Access Control System

The Contractor shall provide, install, configure, test, and commission a complete access control system. The system shall be compatible with the existing access-control environment currently using "AMAG Symmetry," or

shall provide a functionally equivalent/interoperable solution capable of meeting the Government's operational needs as identified in the final solicitation and approved design.

- Provide required servers, workstations, software, licensing, controllers, panels, readers, credentials interfaces, cabling, terminations, and supporting components necessary for a complete system.
- Replace or upgrade designated access card readers and credential readers compatible with existing credentialing requirements, including "HID-compatible readers," where required by the final solicitation.
- Provide handheld credential verification and badge scanner devices functionally equivalent to "Telaeris XPID201" where required by the final solicitation.
- Configure user access levels, permissions, credential functions, audit capability, alarm/event functions, and centralized administration as required for Government operations.
- Integrate access control functions with gate controls, designated entry points, and related electronic security components as required by the approved design.
- Demonstrate successful operation of all access-control functions during Contractor testing and Government acceptance testing.

5.3 Video Surveillance System / Video Management Platform

The Contractor shall provide, install, configure, test, and commission a complete video surveillance system and video management software platform capable of integrating with, or providing functionality comparable to, the existing environment currently using "Milestone Professional+." The system shall provide the functionality required by the final solicitation and approved design while complying with applicable supply-chain, cybersecurity, and installation requirements incorporated into the contract.

- Provide cameras, recording and storage capability, VMS software, licensing, servers or recording appliances, workstations, monitors, cabling, mounting hardware, networked components, and other required system components.
- Provide NDAA-compliant camera units and related components where required by applicable law, regulation, and the final solicitation.
- Provide centralized monitoring, video recording, playback, user permissions, retention settings, camera naming, and event review capability consistent with the approved design.
- Use existing pathways only where suitable, serviceable, authorized, and approved by the Government.
- Maintain logical separation from Government enterprise network equipment unless expressly authorized in writing by the Government.
- Implement required cyber hygiene, system hardening, account management, standalone network, and configuration documentation requirements identified in the final solicitation and approved design.

5.4 Electronic Security System Integration

The Contractor shall integrate the access control, video surveillance, gate control, security monitoring, and related electronic security components into a complete and operable ESS. The integrated system shall support Fort Norfolk security operations and shall be tested as a complete system, not merely as isolated components.

- Verify compatibility and interoperability among installed components.
- Perform system startup, configuration, calibration, commissioning, and functional testing.
- Resolve integration issues before requesting Government acceptance testing.
- Provide a complete configuration record documenting system settings, component inventory, licensing, network/system architecture, and administrative configuration as allowed by the final security review and contract requirements.
- Provide training and turnover support for designated Government personnel.

5.5 Perimeter Fencing, Gates, Gate Operators, and Controls

The Contractor shall replace or upgrade designated perimeter fencing, vehicle gates, pedestrian gates, gate operators, controls, safety devices, sensors, and remote operating devices necessary to support Fort Norfolk access control and perimeter security requirements. Final locations, dimensions, quantities, site constraints, and detailed requirements will be identified in the final solicitation, approved design, site visit documentation, or approved submittals.

- Provide fencing, gates, operators, controls, safety devices, sensors, remote operating devices, mounting hardware, foundations/supports, and related components necessary for a complete and operable installation.
- Ensure gate operators and controls interface with the access-control and entry-control requirements identified in the final solicitation and approved design.
- Provide remote operation capability and operating devices where required by the final contract documents.
- Perform demolition, removal, installation, adjustment, testing, cleanup, and restoration necessary to complete the work.
- Comply with applicable UFC, installation security requirements, manufacturer requirements, approved submittals, and final contract documents.

5.6 Testing, Commissioning, and Acceptance

The Contractor shall test each component, subsystem, and integrated function before requesting Government acceptance testing. Testing shall verify installation quality, functionality, interoperability, performance, recording/playback capability, access-control functions, gate operation, safety devices, and other requirements identified in the final solicitation.

- Submit written test procedures before testing when required by the contract.
- Conduct Contractor quality-control testing before Government acceptance testing.
- Document test results, deficiencies, corrective actions, and retest results.
- Support Government acceptance testing and demonstration of critical system functions.
- Correct all critical deficiencies before final acceptance.

5.7 Training

The Contractor shall provide training to designated Government personnel before final acceptance unless otherwise approved by the Government. Training shall cover system operation, routine administration, access-control management, credential/user management, video surveillance functions, recording and playback, alarm/event review, basic troubleshooting, and maintenance coordination. The Contractor shall provide training materials and attendance records as required by the contract.

5.8 Documentation and Closeout

The Contractor shall provide complete, accurate, and usable documentation necessary to support Government operation and maintenance of the system. Documentation shall be submitted in electronic format and, when required, hard copy format. Closeout documentation shall be approved before final acceptance.

- Approved submittals and product data.
- Shop drawings and as-built drawings/documentation.
- System configuration documentation, subject to security review and final contract requirements.
- Operating manuals and maintenance manuals.
- License information and warranty documentation.
- Test procedures, test results, punch list records, and corrected retest results.
- Training materials and training attendance records.
- Final component inventory and turnover package.

5.9 Warranty and Maintenance Support

The Contractor shall provide warranty support for installed equipment, software, workmanship, and system functionality in accordance with the final solicitation and resulting contract. Preventive maintenance, quarterly maintenance, software support, licensing support, or extended maintenance shall be provided only if required by the final contract documents. The Contractor shall identify warranty terms, maintenance limitations, support procedures, and escalation contacts in the closeout package.

5.10 Service Contract Reporting

If applicable to the final contract type, threshold, and clause structure, the Contractor shall submit required service contract reporting in accordance with FAR subpart 4.17 and the resulting contract. The final solicitation will identify any applicable reporting requirements.

PART 6 - APPLICABLE PUBLICATIONS AND REQUIREMENTS

The following publications and requirements may apply to the final requirement to the extent incorporated into the solicitation and resulting contract. The list is provided for planning and market research purposes and may be revised by the Government before solicitation.

- AR 190-13, The Army Physical Security Program.
- UFC 4-021-02, Electronic Security Systems.
- UFC 4-022-03, Security Fences and Gates.
- EM 385-1-1, U.S. Army Corps of Engineers Safety and Health Requirements Manual.
- Applicable OSHA, Federal, state, local, and installation safety requirements.
- FAR 52.236-13, Accident Prevention, if included in the final solicitation and resulting contract.
- Applicable installation access control requirements and local Fort Norfolk security policies incorporated into the final contract.
- Applicable cybersecurity, supply-chain, information protection, AT/OPSEC, badging, and training requirements incorporated into the final solicitation and resulting contract.
- Applicable NDAA, DoD, Army, and USACE restrictions on covered telecommunications, video surveillance equipment, and supply-chain risk, if incorporated into the final solicitation and resulting contract.

PART 7 - DELIVERABLES

No.	Deliverable	PWS Ref.	Due / Frequency	Format	Submit To
A.001	Quality Control Plan	1.8	Within 10 calendar days after award; updates as needed	Electronic PDF / editable format if requested	KO through COR
A.002	Project Work Plan / Schedule	5.1	Before start of work; updated as needed	Electronic	COR
A.003	Installation Access Roster / Access Log	1.12	Before site access; updated when personnel change	Electronic	COR
A.004	Accident Prevention Plan and AHAs	1.15	Before physical work begins; updated as needed	Electronic PDF	KO through COR
A.005	Submittals, Product Data, and Shop Drawings	5.2-5.5	As required by approved schedule	Electronic	KO/COR
A.006	System Test Procedures	5.6	Before applicable testing event	Electronic	COR
A.007	System Test Results and Deficiency Log	5.6	After testing events; updated through acceptance	Electronic	COR
A.008	Training Plan / Training Materials	5.7	Before training	Electronic	COR
A.009	Training Attendance Records	5.7	After training	Electronic	COR

No.	Deliverable	PWS Ref.	Due / Frequency	Format	Submit To
A.010	As-Builts, O&M Manuals, Warranty Records, and Closeout Package	5.8-5.9	Before final acceptance	Electronic and hard copy if required	KO through COR
A.011	Maintenance Plan / Warranty Support Procedures	5.9	Before final acceptance; if required by contract	Electronic	COR
A.012	Service Contract Reporting	5.10	If applicable	SAM.gov or as required by contract	KO/COR

PART 8 - PERFORMANCE REQUIREMENTS SUMMARY (PRS)

Performance Objective	Standard	Acceptable Quality Level / Threshold	Method of Surveillance
Project Management and Coordination	Contractor manages schedule, submittals, site coordination, deficiency tracking, and closeout activities.	Required plans submitted on time; schedule kept current; no unresolved critical coordination failures.	Document review, meeting participation, COR observation.
Access Control System	System is installed, configured, integrated, tested, and operational in accordance with approved submittals and contract requirements.	No critical deficiencies at acceptance; required components installed and demonstrated.	Submittal review, inspection, functional testing, acceptance testing.
Video Surveillance System / VMS	System is installed, recording, viewable, manageable, and operational in accordance with approved submittals and contract requirements.	No critical deficiencies at acceptance; required recording, playback, viewing, and user functions demonstrated.	Inspection, demonstration, test records, acceptance testing.
ESS Integration	Access control, VSS, gate controls, and related ESS components operate as an integrated system where required.	Integrated functions demonstrated; critical integration deficiencies corrected before acceptance.	Functional testing, acceptance demonstration, deficiency verification.
Fence, Gates, Operators, and Controls	Designated fencing, gates, operators, controls, safety devices, and related components are installed and function as intended.	No critical deficiencies at acceptance; gates/operators and safety devices function as required.	Inspection, operational testing, punch-list verification.
Security, Access, and Information Protection	Contractor complies with contract-incorporated access, training, badging, information protection, and cybersecurity requirements.	No unauthorized access; required training/access documentation submitted when required.	Document review, COR observation, Government access verification.
Safety	Contractor performs work safely in accordance with contract-incorporated safety requirements.	Required safety documents accepted before physical work; unsafe conditions corrected promptly.	Safety documentation review, site observation, deficiency tracking.
Training and Closeout Documentation	Government personnel receive training; required manuals, test records, as-builts, warranties, and closeout documents are submitted and accepted.	All required closeout documents received and accepted before final acceptance.	Document review, attendance verification, closeout review.

PART 9 - ACCEPTANCE CRITERIA

Government acceptance shall occur only after the Contractor has completed installation, integration, testing, commissioning, training, documentation, deficiency correction, and closeout requirements to the satisfaction of the Government. At a minimum, the following criteria must be satisfied before final acceptance:

- All required equipment and materials are installed in accordance with approved submittals, manufacturer requirements, applicable standards, and final contract documents.
- Access control, video surveillance, gate controls, fencing/gates, and related systems function as intended.
- Integrated system functions have been demonstrated successfully.
- No critical deficiencies remain open at the time of acceptance.
- Required training has been completed and documented.
- Required manuals, as-built documentation, test records, warranty information, licensing information, and closeout materials have been provided and accepted.
- All security, access, safety, information protection, and cybersecurity requirements incorporated into the contract have been satisfied for the work performed.

PART 10 - Pre- Solicitation RESPONSE FOCUS AREAS

For interested sources should describe their capability to perform the anticipated requirement. The Government is especially interested in responses addressing the following areas:

- Experience furnishing, installing, integrating, testing, commissioning, and maintaining electronic security systems at Federal, DoD, Army, USACE, or similarly secured facilities.
- Experience with physical access control management systems compatible with an existing environment using "AMAG Symmetry" or functionally equivalent/interoperable systems.
- Experience with access card readers / credential readers compatible with existing credentialing requirements, including "HID-compatible readers."
- Experience with handheld credential verification and badge scanner devices functionally equivalent to "Telaeris XPID201."
- Experience with video surveillance systems and VMS platforms capable of integrating with or providing functionality comparable to "Milestone Professional+."
- Experience with perimeter fencing, gates, gate operators, safety devices, sensors, and access-control integration.
- Experience complying with cybersecurity, supply-chain, information protection, installation access, safety, and security requirements applicable to Federal security-system installations.
- Ability to perform as a prime contractor and the approximate percentage of work the firm would perform with its own employees.
- Recommended NAICS code, acquisition considerations, commercial practices, lead times, supply-chain constraints, and other market information the Government should consider.

PART 11 - DRAFT PWS LIMITATIONS

This draft PWS is provided for the Pre-Solicitation only. It does not represent the final requirement. The Government reserves the right to revise the scope, performance requirements, quantities, technical standards, acquisition strategy, brand-name/brand-name-or-equal approach, security requirements, cybersecurity requirements, clauses, wage determinations, evaluation criteria, and contract type before issuing any solicitation. Nothing in this draft PWS obligates the Government to issue a solicitation or award a contract.