Performance Work Statement

1 Scope

This Performance Work Statement (PWS) defines the services needed by the Transportation Security Administration's (TSA) to implement the TSA Gold+ initiative. The TSA Gold+ requires a complete, turnkey solution to deliver and manage both security screening technology and a skilled workforce capable of screening passengers and their property at participating airports for explosives, weapons, and other prohibited items.

1.1 Background

The mission of TSA is to protect the Nation's transportation systems to ensure freedom of movement for people and commerce. In support of this mission, the Screening Partnership Program (SPP) was established under Congressional mandate through the Aviation and Transportation Security Act (ATSA) of 2001 and amended by subsequent laws, including the FAA Modernization and Reform Act of 2012, and the FAA Reauthorization Act of 2018. Under SPP, screening of passengers and property at participating airports is performed by a private, contracted screening workforce under Federal oversight.

TSA screens nearly 2.5 million passengers daily across more than 400 commercial airports, and passenger volumes are projected to continue growing. Historically, TSA's dual role as operator and regulator has established a strong foundation of security and operational standards. TSA Gold+ creates the opportunity to build on that foundation - unlocking greater agility, investment, and innovation. In alignment with Administration priorities and executive orders, TSA is working to restore the Golden Age of Travel and reassert America's global dominance in aviation security and innovation. TSA Gold+ is a transformative initiative designed to modernize aviation security by empowering airports to opt-in to a privatized screening ecosystem tailored to their unique operational and community needs. Building on the Screening Partnership Program (SPP), TSA Gold+ reimagines public-private partnerships to accelerate the adoption of cutting-edge technologies and operational solutions that enhance security, efficiency, and passenger experience.

1.2 Overview

TSA Gold+ aims to redefine the relationship between TSA, airports, and industry by transitioning TSA's role from both operator and regulator to security regulator providing oversight at the selected airports. This shift allows private industry to operate checkpoints under TSA oversight, creating space for enhanced security, innovation, and operational excellence. The program introduces turnkey solutions that integrate advanced technologies, privately managed screening personnel, and tailored security ecosystems to meet the specific needs of airports.

The objectives of TSA Gold+ are to:

- **Elevate Customer Experience:** Deliver a seamless, efficient, and user-friendly journey for travelers by integrating advanced technologies, increasing capacity and throughput, and

providing personalized services that enhance overall satisfaction and confidence in aviation security.

- **Accelerate Innovation:** Enable rapid deployment of cutting-edge technologies to enhance security effectiveness and passenger throughput.

- **Drive Investment:** Attract private-sector funding to modernize security infrastructure, reduce taxpayer burden and unlock new market opportunities for aviation security innovation.

- **Enhance Security:** Ensure that operators meet or exceed the same outcome-based security metrics used by TSA through robust oversight of screening operations, including oversight of threat detection, cybersecurity and operational resilience.

- **Enable Airport Choice**: Empower airports to actively participate in designing and informing operational requirements through a flexible public-private partnership framework, ensuring solutions are tailored to local needs and security priorities.

- **Improve Flexibility:** Allow airports to customize their operations, fostering greater collaboration between TSA, industry, and local communities.

TSA Gold+ gives airports a new pathway to work with TSA and industry partners to modernize security operations by using contracted screening services, deploying next generation Transportation Security Equipment (TSE), and designing bespoke curb-to-gate experiences. The program is designed to accommodate airports of all sizes and layouts, ensuring scalability and adaptability to dynamic operational needs. TSA will maintain robust regulatory oversight to ensure compliance with outcome-based security metrics, while collaborating with private industry to drive innovation and operational excellence.

1.3 General Requirements

This section defines the Offeror's general requirement for responsibilities that apply to this Contract.

1.3.1 Performance Requirements

The Offeror shall meet or exceed the general performance requirements in this section.

1.3.1.1 Standards and Code Requirements

The Offeror shall ensure that all work performed is in compliance with all applicable local, state, and federal standards, codes, and regulations, including obtaining any required licenses, permits, approvals, and authorizations. (See Attachment J – SPP, 35 SAFETY ACT BLOCK DESIGNATION NOTICE)

1.3.1.2 Security Clearance and Sensitive Security Information (SSI)

All personnel[1] are required to go through an STA[2] (Security Threat Assessment) and receive a favorable TSA suitability determination prior to commencing work on this requirement. (See Attachment J – SPP, 38 Suitability Determination)

Most of the information that the Offeror will encounter during the performance of the requirement will be Sensitive Security Information (SSI). All material marked SSI shall be handled according to TSA policy, guidance and procedures.

For those orders that require access to classified information (up to the SECRET level) personnel will be required to be vetted via TSA's process for clearance. TSA does not anticipate requiring the handling and storage of classified information (up to the SECRET level) at the Offeror's facility. TSA will provide access to TSA's classified processing and storage facilities on an as needed basis. (See 18 Attachment C - SSI Policies and Procedures Handbook)

1.3.1.3 Off Hour Communication

Tasks completed under this contract will be performed within and outside of the normal Government business hours of Monday through Friday, 8am and 5pm (EST). Any challenges with screening operations, personnel safety, maintenance, and/or equipment installations/upgrades, should be communicated within 1 hour of incident to the Contracting Officer's Representative (COR)/Technical Monitor (TM) or airport designee.

1.3.1.4 Subcontractor Management

The Offeror shall flow down all applicable requirements to subcontractors for compliance with the overall performance Contract. The Offeror shall review each subcontractor's technical progress on all assigned tasks and include such technical progress and status information in reporting requirements. The Offeror shall inform the Government in advance of any anticipated disruption of services resulting from conflicts or disputes with subcontractors and partners, strikes, or any other occurrences that may cause disruption of work. The Offeror is responsible for establishing all Non-Disclosure Agreement (NDA) with subcontractors to ensure data and Intellectual Property (IP) are protected.

1.3.1.5 Data Retention

All data retention, handling, and disposition by the Offeror must be in full compliance with all applicable TSA regulations, federal, state, and local laws, and TSA policies regarding privacy, data protection, and information security. The Offeror shall retain all data generated under this Contract and its orders until the expiration of the Contract. Upon Contract closeout, all data (including reports, test data sheets, analysis data, and all other documents collected or generated)

---

[1] Foreign nationals require an alternate process set forth in TSA MD 2810.3, Management of Foreign Access to Sensitive Information, https://ustsa.sharepoint.com/sites/DirectivesandForms/Policies/Policies%20Library/TSA%20MD%202810.3,%20FINAL,%20180625.pdf

[2] In addition to an STA, potential offerors are typically required to provide 1) a certification from each company/entity that its employees/personnel who are provided access to SSI are properly trained; 2) an NDA for each individual who is granted access to SSI; and 3) an affirmation that each company/entity will designate a Senior Official who can certify that all appropriate protections will be followed, only authorized individuals will have access to the sensitive information, and that those individuals adequately understand their responsibilities to protect the information

shall be provided to TSA in a format and medium specified by TSA. TSA may require some of the data to be deleted after backup to TSA is complete.

1.3.1.6 Data Rights

TSA encourages all Offerors to propose innovative solutions using data produced under the Operations Management Plan (OMP). However, the parameters for use of the screening data that will be produced under the OMP are governed by various federal statutory, regulatory, and policy prohibitions on use. Accordingly, data first produced by a screening solution under the OMP shall be produced under FAR 52.227-17. Such data shall include, but is not limited to, reports, Field Data Reporting System (FDRS) info related to system and officer performance, configuration, analytic or screening outputs (including all imagery and metadata), and all raw data including the attenuation measurements from the high and low detectors that are used for determination of the effective atomic number, Zeff and density (ρ) and image data that is defined as the image information generated after raw data has been processed by any of the screening systems.

COTS software or pre-existing proprietary platform software is not considered data produced under this contract. Software modifications developed specifically for the contract after award, including algorithm software, and configuration artifacts created using Government data or data first produced under this contract are encouraged. However, modification of all proprietary or COTS software utilized in the performance of this contract must be approved by TSA before implementation under the OMP. The implementation of emerging technologies based on data produced through the performance of the TSA Gold+ initiative shall be implemented through negotiated permission for use and/or incorporation of such data or the derivative product of such data into novel technology products, including derivative software products modified or created through the use of data produced under this contract. This implementation of emerging technologies is expected to be complementary to the implementation of turnkey technology solutions as described under section 1.5.2.1. of this PWS. The Offeror is responsible for providing appropriate licensing to the Government, for the Government to access and evaluate any software (COTS or otherwise) to be used under the OMP or provided for evaluation under 1.5.2.1. or 1.5.2.2 of this PWS. The Government expects that derivative data products of proprietary or COTS solutions modified using data produced under the performance of this contract shall be delivered to the government under FAR 52.227-14 Data Rights, Alt II or III, depending on the format of the data.

TSA retains, and the Offeror does not acquire, data rights to any Government furnished information. For the sole purpose of work under this Contract and no other, TSA may provide its owned or licensed data ("TSA Data") to the Offeror during the Engagement. TSA warrants that it has all necessary rights to share TSA Data with the Offeror as described herein. TSA Data includes all data collected, processed, developed by TSA, or collected directly by the Offeror while performing a TSA contract function. TSA Data shall continue to be owned by TSA, and Offeror will not retain TSA Data beyond the end of the Contract and will always maintain such TSA Data as confidential under this Contract. The Offeror may use TSA Data to perform development, testing and analytical tasks and to create outputs generated by applying advanced technologies. The Offeror may use, both during and after this Contract, improvements to advanced technologies that were created based on learnings from this Contract. Any such use of improvements must not

involve retention or reuse of TSA Data itself, except as expressly authorized by TSA. All use, handling, and sharing of TSA Data by the Offeror must comply with all applicable federal, state, and local laws, including but not limited to privacy, data protection, and information security requirements. (See 19 Attachment D – ITAR_Terms-Conditions GOLD+)

1.3.1.7 Facilities and Office Space

The Offeror shall be responsible for obtaining and funding any office, administrative, warehouse or staff support space (including break rooms and locker areas) required to support Gold+ operations, unless TSA or the airport authority explicitly provides such space in the task order. Any use of TSA or airport provided space shall be governed by local agreements, and the Offeror shall comply with all associated rules, security requirements, and access controls.

1.3.2 Excluded Services

The Offeror is not responsible for providing or managing TSA Canine (K9) teams or Transportation Security Specialist-Explosives (TSSE) personnel, or TSA Inspectors as part of this contract. These functions will remain the responsibility of TSA Federal resources. The Offeror shall coordinate with TSA for any operational scenarios or incidents that require K9 or TSSE support, but shall not plan, staff, or deliver these services under Gold+.

1.4 Program Management

This section defines the Offeror's responsibilities for program management and oversight of all Gold+ airport operations.

1.4.1 Objective

The Offeror shall provide comprehensive program management to meet the performance objectives outlined in this Performance Work Statement (PWS) for aviation security screening services and technology solutions at designated Gold+ airports.
Program management shall support TSA's regulatory oversight role and enable continuous improvement, innovation, and tailored solutions to meet the needs of airports, airlines, passengers, and communities.

1.4.2 Performance Requirements

The Offeror shall provide program management support that meets or exceeds the performance requirements in this section.

1.4.2.1 Program Management

The Offeror shall establish and maintain robust management processes to oversee all aspects of Gold+ airports including program management, financial management, workforce management, maintenance of technology and equipment, equipment and materials management, risk management, cybersecurity, customer service, quality control, health and safety, and subcontractor

management. The Offeror shall ensure compliance with TSA statutory requirements, directives, standards, and performance objectives.

1.4.2.2 Key Personnel

The Offeror shall designate a qualified Operations/Program Manager and a Deputy Operations/Program Manager as key personnel and the primary points of contact for TSA. The Operations/Program Manager and its Deputy shall be responsible for overall operational performance, coordination with TSA, and implementation of contract requirements.

The Program Manager shall have a minimum of 15 years of program management or equivalent demonstrated experience and ten (10) years specializing in managing similar Federal programs (similar size and complexity). A bachelor's degree or equivalent certifications are required. The Program Manager shall have relevant experience in any of the following fields: aviation security, airport operations personnel security screening services, equipment management, or contract management. Information Technology (IT) and screening operations experience is preferred to include knowledge of Government processes such as obtaining an Authority to Operate (ATO) and screening processes and procedures. If an employee lacks such experience, the Offeror, by written request, shall provide evidence of similar/equivalent experience. Acceptance of evidence shall be at discretion of the Contracting Officer (CO)/Representative (COR). The Deputy Program Manager shall have a minimum of 10 years of program management experience and five (5) years specializing in managing similar Federal programs (similar size and complexity).

Additional key personnel shall be identified as required to support operational, technical, and transition activities at the task order level. Potential key management team personnel could include a Project Manager, Lead Engineer, Security Training Instructor, and Transition Manager. Any changes to key personnel must be approved by TSA in advance.

1.4.2.3 Operations Management Plan

The Offeror shall develop, implement, and maintain an Operations Management Plan (OMP) that addresses all aspects of contract performance. The OMP shall be updated as needed to reflect changes in TSA requirements, operational needs, or lessons learned. The Offeror shall consider including the following key elements but is not limited to the list below:

i. Staffing: Recruitment, onboarding, scheduling, attire, clearances, qualifications, fitness for duty, incident and emergency management, claims management, technology implementation maintenance, and reporting, and management of personnel to meet TSA operational requirements. The OMP shall also address surge staffing capabilities for both onsite screening functions and TSA directed remote image review, including how the Offeror will identify, train, and deploy additional personnel to support peak periods, special events, irregular operations, and centralized or remote screening missions, while maintaining required qualifications and clearances.

ii. Training: Initial and recurrent training, certification, and professional development to ensure all personnel meet TSA standards and are qualified for their assigned roles. (See Attachment J – SPP, 37 TRAINING REQUIREMENTS)

iii. Equipment Management: Site management, procurement, delivery, testing, and acceptance, systems integration, cybersecurity, configuration management, maintenance, logistics, property management, safety, storage, and disposal of security screening equipment, Information Technology (IT) / Operational Technology (OT), peripheral solutions, and consumables needed to effectively screen passengers and baggage to include both accessible property/carry-on and checked baggage. (See Attachment J – SPP, 36 ESTIMATED CONSUMABLES LIST)

iv. Uniform Management: Procurement, issuance, maintenance, replacement, and enforcement of uniform standards to ensure all personnel are properly attired in accordance with TSA requirements and operational guidelines. (See 25 Attachment H - TSA Handbook 1100.73-2, FINAL, 201218)

v. Risk Management: Processes and procedures to identify, assess, and manage potential risks including escalation of priority risks and issues.

vi. Quality Control: Methods, procedures, and metrics used to monitor and ensure compliance with all contract requirements and TSA performance and customer service/hospitality standards including address inspection, testing, and corrective actions.

vii. Financial Viability: Approach to leverage private sector investment and expertise to support the Gold+ mission, including methods for ensuring ongoing financial health (i.e. revenue streams, operating costs, capital expenditures, etc.), reinvestment planning (infrastructure upgrades, technology refreshes, etc.), benchmarking against industry standards, and sustainable capital management.

Offerors shall demonstrate sufficient capitalization and financial resilience to support integrated staffing, technology deployment, sustainment, and reinvestment over the proposed period of performance. Proposals may include reinvestment plans, technology refresh strategies, and sustainable capital management approaches that improve long-term performance and reduce taxpayer risk.

viii. Continuous Improvement/Optimization Efforts: Processes and procedures to identify, assess, and propose improvements to PWS components for TSA consideration. Partner with TSA to implement approved proposals.

The Offeror may propose expanding on key elements of the OMP in additional documents as appropriate. The OMP shall be submitted for TSA approval and updated as directed.

1.4.2.4 Reporting and Communication

The Offeror shall provide timely, accurate, and professional status reporting as listed in the Checkpoint Requirements and Planning Guide (CRPG) or as otherwise specified by TSA that include operational summaries, airport and equipment reports, performance management reviews, incident and security reporting, claims summaries, employee and clearance summaries, and transition reports (as applicable). The Offeror shall track and report compliance with the OMP. The Offeror shall maintain open and effective communication with TSA and airport stakeholders (i.e. Federal Security Director (FSD) or designee) at a cadence determined by the Offeror and

COR. The Offeror shall be prepared for more frequent meetings, ad-hoc reports, and reviews during transition periods or if performance or operational issues arise at TSA request.

1.4.2.5 Risk Management and Quality Control

The Offeror shall proactively identify, assess, and mitigate risks that could impact security, operations, or customer service. TSA COR and the FSD has to be notified in advance and provide approval for new plans implementation. The Offeror may implement a Risk Management Plan (RMP) separately from the OMP that describes the risk management methodology. The Offeror shall implement quality control measures to ensure compliance with contract requirements and TSA standards outlined in the Performance Requirements Summary. The Offeror may implement a Quality Control Plan (QCP) separately from the OMP that describes the methods, procedures, and metrics used to monitor and ensure compliance with all contract requirements and TSA performance standards.

TSA will monitor Offeror performance in accordance with the Government's Quality Assurance Surveillance Plan (QASP). The Offeror shall cooperate fully with TSA's quality assurance activities, including inspections, audits, performance reviews, and requests for information or corrective action.

1.4.2.6 Continuous Improvement and Innovation

The Offeror shall foster a culture of continuous improvement, leveraging data, best practices, and stakeholder feedback to enhance security outcomes, operational efficiency, and customer experience. The Offeror is encouraged to propose and implement innovative solutions, subject to TSA approval.

1.5 Technology Solution Implementation

This section defines the Offeror's responsibilities for technology solution implementation at Gold+ airports.

1.5.1 Objective

The Offeror shall deliver, install, integrate, test, and maintain turnkey security screening technology solutions at designated Gold+ airports to support effective, efficient, and compliant screening operations. Technology solutions shall meet or exceed TSA standards for performance, reliability, cybersecurity, and operational availability.

1.5.2 Performance Requirements

The Offeror shall provide technology solution implementation support that meets or exceeds the performance requirements in this section.

1.5.2.1 Turnkey Technology Solutions

The Offeror shall deliver, install, and integrate turnkey security screening equipment, Information Technology (IT) / Operational Technology (OT) systems, peripheral solutions, consumables, and

associated Furniture, Fixtures, and Equipment (FFE) that are specified on the Acceptable Capabilities List (ACL) , found at www.tsa.gov/sites/default/files/cap_acceptable_capability_list.pdf (See 20.1 Attachment E - cap_acceptable_capability_list) or have been tested and approved by TSA for use. Solutions shall be operationally ready, fully functional, and compliant with all applicable TSA technical and regulatory requirements. The Offeror shall ensure the provided capabilities use the most up-to-date configuration, including the components, parts, software, and related materials, provided and approved by TSA. Any changes to the TSA-approved configurations (to include system updates, and changes to hardware, software, etc.) and subsequent timelines of installation and implementation must be approved by TSA prior to implementation. Additional testing may be required for any changes to the configuration. TSA may permit phased deployment and evaluation of emerging technologies through pilot implementations documented in advance through agreements such as CRADAs, prior to full-scale operational deployment, provided security efficiency, effectiveness and TSA performance requirements are maintained. (See 24 Attachment G – TSA T&E Guidebook Rev 6 – Final)

The Offeror shall deliver and install the necessary infrastructure required to support security screening equipment. This may include power, ethernet cables, fiber cables, and other peripheral equipment in accordance with the Checkpoint Requirements Planning Guide (CRPG).

The Offeror shall support TSA's open architecture objectives to enable modular, interoperable, and standards-based solutions. The Offeror shall define a data management approach in which data will be (1) accessible to TSA and applicable subcontractors except when limited by security, policy, or regulations and (2) transmitted through well and openly defined interfaces to the maximum extent possible.

1.5.2.2 IT Architecture and Technical Standards

The Offeror shall ensure that all Information Technology (IT) and Operational Technology (OT) components used to support Gold+ operations conform to TSA's Screening Reference Architecture, Enterprise Architecture, and Technical Standards Profiles (TechSP), as applicable. This includes, but is not limited to, operating systems, databases, middleware, network devices, and security tools.

All proposed IT/OT solutions (including vendor owned or leased systems) that connect to TSA networks, process TSA Data, or interface with TSA systems shall:

- Use TSA approved or TSA compatible technology stacks (e.g., approved operating systems, network platforms, and security controls) as defined in the TechSP and other TSA IT standards;

- Be interoperable with TSA's existing infrastructure and services (e.g., Secure Flight, AIM, Performance Measurement Information System - PMIS), using TSA approved protocols and interface specifications; and

- Be documented in architecture and design artifacts (e.g., network diagrams, interface control documents) submitted to TSA for review and approval prior to implementation.

- Ensure future interoperability with TSA's Threat Recognition System (TRS), maintain robust TSA connectivity, and support open architecture—enabling modular, standards-based solutions that facilitate integration with evolving TSA systems and third-party technologies.

If the Offeror proposes the use of technologies or platforms that deviate from TSA's approved standards, the Offeror shall identify those deviations and request written approval (or waiver) from TSA in advance. Approval of such deviations is at TSA's sole discretion.

The applicable Screening Reference Architecture, Enterprise Architecture artifacts, and Technical Standards Profiles (TechSP) will be provided as Government Furnished Information (GFI) upon request or as part of the solicitation package.

1.5.2.3 Site Preparation and Installation

The Offeror shall conduct site surveys, prepare installation designs, and coordinate with airport and TSA stakeholders to ensure timely and effective deployment of technology solutions. The Offeror shall consider the necessary infrastructure, electrical, data, and other relevant design components or airport-specific requirements. TSA will make the Checkpoint Requirements and Planning Guide (CRPG)[3] and the Planning Guidelines and Design Standards (PGDS) for Checked Baggage Inspection Systems available as a reference to support site preparation. The Offeror shall provide Site Design and Installation Plans and As-Built Designs for each Gold+ airport for TSA approval prior to implementing any solutions. (See Attachment F – checkpoint-requirements-and-planning-guide).

If existing equipment is to be decommissioned, the Offeror may be asked to provide the necessary services to decommission, relocate and/or remove, package, and ship to a Continental United States (CONUS) location determined by TSA. For decommissioning or moving TSA owned equipment or infrastructure, the Offeror shall follow TSA property management procedures[4]. The Offeror is responsible for safeguarding TSA property at all times and fully liable for any damage or losses, until TSA takes possession in shipment, warehouses, manufacturer's depot, and/or loading/unloading to/from site locations including installations/decommissions, as applicable.

Site preparation, installation and decommission of solutions shall minimize disruption to airport operations and comply with all safety and security requirements.

1.5.2.4 Configuration and Integration

The Offeror shall ensure all equipment and systems are configured, integrated, and tested according to TSA-approved specifications. The Offeror shall track and manage the configuration (including major systems, subsystems, components, hardware, and software) of all technology assets throughout their lifecycle and across multiple development and production baselines. The Offeror shall provide Configuration Status Accounting Reports providing accurate configuration data for each system. Any changes to system configuration shall be subject to TSA approval and

[3] The Offeror cannot provide a solution that is non-compliant to CRPG

[4] The Offeror will hire an OEM certified technician to conduct the decommissioning

documented in accordance with TSA configuration management procedures. (See Attachment A - Gold+_CM Req_Attachment_4.13.26)

1.5.2.5 Acceptance Testing

The Offeror shall coordinate and complete all required acceptance testing (e.g., Factory Acceptance Testing, Site Acceptance Testing, Integrated System Acceptance Testing, Network Throughput Testing) in accordance with the most recent TSA-approved test plans and procedures and using TSA-approved third-party agents. The Offeror shall document the results of acceptance testing in an Acceptance Testing Report. Decisions regarding a system passing or failing acceptance testing events are made solely by TSA. The Offeror shall resolve any deficiencies identified during testing prior to operational use.

1.5.2.6 Maintenance

The Offeror shall provide ongoing preventive and corrective maintenance, including cybersecurity updates, warranty handling, radiation surveys, and radioactive leak tests, to ensure equipment and systems meet or exceed TSA-defined operational availability and reliability requirements. The Offeror shall provide supply chain logistics support resources including repair parts, training, tools, and test equipment needed to repair and service the equipment. The Offeror shall provide a Maintenance Report outlining, at a minimum, preventative and corrective maintenance activities completed within the defined period and forecasted expected maintenance needs to keep equipment operational. The Offeror shall maintain trained and certified technicians within reasonable proximity to each airport. The Offeror is responsible for coordinating with TSA to implement solutions for all parts obsolescence issues.

At many Gold+ airports, TSA owned equipment and infrastructure may already be installed and operational at the time of contract award. Effective immediately upon commencement of contract performance, the Offeror shall assume full responsibility for operating, managing, and maintaining all TSA-owned equipment used in support of Gold+ screening operations, otherwise specified in the task order. The Offeror shall be responsible for operating, managing, and maintaining all TSA owned equipment used in support of Gold+ screening operations from the commencement of performance, unless otherwise specified in the task order. If any such equipment becomes inoperable or fails to meet TSA's operational availability standards, the Offeror shall be responsible for repairing or replacing the equipment, in coordination with TSA, using TSA approved solutions. (See Attachment B - Gold+_Maintenance Req_Attachment_4.13.26)

1.5.2.7 Cybersecurity and Data Protection

The Offeror shall ensure all technology solutions—regardless of whether they are TSA owned, airport owned, or vendor owned—comply with TSA cybersecurity policies and requirements, including regular updates, vulnerability remediation, audit logging, and privileged access controls. Any system that processes, stores, or transmits TSA Data or connects to TSA networks is subject to these requirements.

All connectivity-based solutions shall obtain and maintain the appropriate Authority to Operate (ATO) or Authority to Connect (ATC) in alignment with applicable DHS and National Institute of

Standards & Technology (NIST) policies (e.g., NIST SP 80053 controls), the TSA Information System Security Program Policy Directive, and relevant Security Technical Implementation Guides (STIGs). The Offeror shall cooperate with TSA IT for cybersecurity assessments and implement corrective actions as directed, including maintaining and updating Plans of Action and Milestones (POA&Ms) for identified deficiencies.

The Offeror shall comply with all applicable privacy and data protection requirements, including the Privacy Act, DHS/TSA privacy policies, and Sensitive Security Information (SSI) handling rules. Any personally identifiable information (PII), SSI, or other sensitive operational data collected or accessed under this contract shall:

- Be used solely for TSA approved operational and security purposes, as defined in the contract or task order;
- Not be disclosed to third parties or used for independent commercial purposes (e.g., external monetization, targeted advertising) without prior written TSA approval;
- Be protected using TSA approved encryption, access control, and logging mechanisms, and retained only for the period authorized by TSA; and
- Be destroyed or returned to TSA in accordance with TSA media sanitization and data destruction requirements at the conclusion of the contract or when no longer needed.

Any data sharing between TSA systems and vendor owned systems shall occur only through TSA approved interfaces and data exchange mechanisms (e.g., APIs, secure file transfers) documented in interface control documents and approved by TSA. Where possible, operational data used by the Offeror for performance management or innovation proposals shall be aggregated or deidentified, consistent with TSA guidance. TSA retains ownership of TSA Data; the Offeror may not assert proprietary rights over TSA Data and may not retain, share or use such data outside the fulfillment of TSA functions unless expressly authorized by TSA. (See 19 Attachment D ITAR Terms-Conditions GOLD+)

1.5.2.8 Property and Asset Management

The Offeror shall safeguard, track, and manage all technology assets throughout their lifecycle, including installation, operation, maintenance, and disposal, in accordance with TSA property management procedures. The Offeror shall provide an Inventory Report tracking all assets under Offeror management. The following information should be considered as part of property management activities: Manufacturer, Type and Model Number, Value of the Equipment, Acceptance Date, and Serial Number.

1.5.2.9 Continuous Improvement and Innovation

The Offeror is encouraged to propose innovative technology and process solutions at the checkpoint, checked baggage area, and other applicable locations. Potential innovation areas include, but are not limited to, solutions that enhance the TSA PreCheck® experience and further differentiate risk-based trusted traveler screening from standard passenger screening operations. Proposed solutions may include technologies, operational concepts, automation, and passenger

experience enhancements designed to increase efficiency, convenience, throughput, and security effectiveness, including within dedicated TSA PreCheck lanes, while maintaining compliance with TSA security requirements and risk-based screening principles.

When proposing innovative solutions for deployment under a task order, the Offeror shall provide supporting analysis, requirements, testing methodologies, and results to support TSA evaluation of proposed solutions. The approval path for proposed solutions will vary depending on the complexity, maturity, and risk of each proposed solution.

1.6 Security Screening Services

This section defines the Offeror's responsibilities for security screening services at Gold+ airports, including screening operations, compliance, and customer service requirements.

1.6.1 Objective

The Offeror shall provide comprehensive security screening services at designated Gold+ airports to secure passengers, baggage, and airport facilities in accordance with statutory requirements, TSA standards, and performance objectives. The Offeror shall deliver screening services that meet or exceed the level of performance provided by Federal Government personnel.

1.6.2 Performance Requirements

The Offeror shall provide security screening services support that meets or exceeds the performance requirements in this section.

1.6.2.1 Screening Operations

The Offeror shall conduct passenger, baggage, and access control screening at TSA-established Screening shall be performed by fully trained and certified personnel using approved procedures and technologies.

At TSA's direction, the Offeror shall also provide qualified personnel to support remote review and other centralized screening activities, using TSA-approved systems and secure connectivity. Such personnel shall meet all TSA training, certification, and suitability requirements applicable to image interpretation and remote operations. The Offeror shall ensure that surge staffing capacity is available to support these remote image review missions during periods of increased demand or special operations, in coordination with the Federal Security Director (FSD) or designee.

Unless otherwise specified in an individual task order, the security screening operations shall commence no later than two hours prior to the first flight associated with that screening area. Additionally, security screening operations shall cease once the last flight has left the airport (wheels up), unless a formal request is made by the airline for flights that are delayed. The Offeror shall plan to open and close screening locations consistent with this requirement and any modification thereof, as indicated in the task order, due to irregularly departing flights. The Offeror shall perform the following activities, including but not limited to:

i. Screen persons and property entering designated security areas including confirming or resolving alarmed persons or property;

ii. Screen baggage and other items destined for an aircraft or entering designated security areas including confirming or resolving alarmed persons or property;

iii. Prevent persons from entering designated security areas from exit lanes;

iv. Verify travel documents of passengers entering designated security areas for authenticity and required designated markings.

v. Inspection notifications and claims management;

vi. Immediately report all security related issues, incidents, or concerns as outlined herein.

vii. Coordinate with airport and local law enforcement on VIP movements

The Offeror shall ensure adequate staffing for enterprise technology solutions and account for multiple operational scenarios and TSA-directed special screening programs while conducting screening:

i. Screening services during peak and off-peak times including surge staffing during periods of increased demand (i.e. holidays, summer travel);

ii. Screening services for delayed or unplanned commercial passenger flights;

iii. Screening services for planned public charters;

iv. Layered screening activities;

v. Staffing shortfalls caused by inclement weather, personnel readiness issues, and other foreseeable factors;

vi. Emergency and reconstitution events;

vii. DCA Access Standard Security Program (DASSP);

viii. TSA Cares, Passenger Support Specialist Program (PSS);

ix. Advanced Threat Local Allocation Strategy (ATLAS) activities;

x. Risk Emphasized Flight Screening (REFS);

xi. Crew Member Access Program (CMAP);

xii. Law Enforcement Officer Flying Armed (LEOFA) Pass;

xiii. Registered Traveler (RT) program; and

xiv. TSA PreCheck® expedited screening

1.6.2.2 Compliance

The Offeror shall comply with all TSA Standard Operating Procedures (SOPs), directives, and policies, as specified in Government Furnished Information (GFI) provided after award and updated by TSA. The GFI documents may change on a yearly basis or more frequently to incorporate updated and newly created materials. The Offeror shall be responsive to immediately implement security screening-related direction, within the scope of work, upon receipt of such direction from the COR/Technical Monitor and/or Federal Security Director (FSD) or designee during urgent and compelling security events. The Offeror shall ensure all personnel are knowledgeable of and adhere to current TSA requirements. If, during performance, the Offeror identifies potential improvements or efficiencies that are not detrimental to security, the Offeror may submit proposed SOP adjustments or new SOPs to TSA for review and written approval prior to implementation.

Compliance with TSA requirements will be monitored through defined compliance metrics, which are integral to the Performance Requirements Summary and will be used to assess the Offeror's adherence to SOPs, training, maintenance, cybersecurity, and other critical obligations.

1.6.2.3 Operational Outcomes

In accordance with 49 U.S.C. §44920, the level of screening security services and protection provided under Gold+ shall be equal to or greater than the level that would be provided by Federal Government personnel. Failure to perform equal to or greater than the level that would be provided by Federal Government personnel will result in Government action up to and including contract termination. Corrective actions and associated escalations are outlined in the Performance Requirements Summary. The Offeror shall achieve and maintain performance standards for throughput, alarm resolution, wait times, and customer service as specified by TSA in the Performance Requirements Summary. The Offeror shall minimize passenger wait times and maximize checkpoint efficiency through effective staffing and technology utilization. The Offeror shall have plans and processes in place to address issues related to achieving the defined performance standards. (See Attachment I – Governance, 27 OD-400-50-1-5H Reporting Customer Thruput-Wait_Times_111220_FINAL_sig)

1.6.2.4 Incident Management and Continuity of Operations

The Offeror shall promptly report all security incidents, anomalies, and concerns to TSA in accordance with established procedures. Reportable incidents are considered any issue that may impact security, regulatory compliance, or public perception. Written incident reports shall be provided within specified timeframes.

The Offeror shall maintain readiness for emergencies and be responsible for the continuity of operations in the performance of security screening services. The Offeror may implement a Continuity of Operations (COOP) Plan and Exercise Report(s) separately from the OMP with consideration for, but not limited to, employee training and participation, existing airport events/plans, emergency procedures and readiness preparation, and recall / return to operations.

1.6.2.5 Customer Service

The Offeror shall engage with passengers and stakeholders in a professional and courteous manner, promptly addressing inquiries and concerns. The Offeror shall maintain a Customer Service Log and report passenger-related incidents, not otherwise reported as security incidents, and passenger concerns. The Offeror is expected to exercise sound judgment regarding the need for an expeditious verbal or written report, according to the nature of the inquiry. The Offeror shall be responsible for responding to customer experience (CX) inquiries received through the TSA Contact Center or local stakeholder manager, in accordance with TSA protocols and guidance. The Offeror shall immediately present inquiries to TSA when:

i. Incidents involve security, regulatory, or organizational matters under TSA discretion;

ii. Coordination with the FSD or designee or TSA Headquarters is needed to provide a response;

iii. Allegations of improper security screening procedures;

iv. Civil rights issues or the alleged discrimination by Offerors against passengers or any TSA regulated party is involved;

v. A member of Congress or DHS/TSA senior leadership is notified, and/or believed to be aware of the inquiry;

vi. A TSA legal response, an opinion, or statement of position is requested;

vii. Inquiries involving an allegation of criminal activity or significant misconduct by the Offeror workforce, or any incident as identified by the FSD or designee that involves the Offeror workforce; and

viii. Inquiries are from the media or may result in media attention.

Once the offeror informs TSA, TSA will make the determination as to whether the Offeror or TSA will respond to the inquiry. The Offeror shall answer TSA questions and support fact finding for matters related to the scope of the contract as needed. The offeror shall follow TSA Management Directive 900 Compliments and Complaints. TSA and the Offeror are expected to work collaboratively in this process.

1.6.2.6 Claims and Property Management

The Offeror shall manage passenger and baggage claims, lost and unclaimed property, voluntarily abandoned property, and hazardous materials in the purview of the security checkpoint in accordance with TSA policy and applicable law. The Offeror may implement a Claims Management Plan separately from the OMP to explain the processes and procedures the Offeror will use to document, address, and resolve passenger claims related to the security screening services and baggage handling, within 60 days from claim receipt. Additionally, the Offeror shall consider appeals procedures and claims for lost or damaged personal property as well as claims

for personal injury or wrongful death. Claims information shall be held by the Offeror for a minimum of two years following the resolution of the claim. (See Attachment I – Governance)

While the TSA wants to ensure that claims of passengers at airports are dealt with fairly and promptly, the resolution of passenger and baggage claims is a matter of state law and must be resolved between the Offeror and the claimant. If a claimant files a claim with the TSA, it will be referred to the Offeror for processing. The Offeror shall process all passenger and baggage claims in accordance with the OMP or Claims Management Plan and applicable state tort law.

1.6.2.7 Continuous Improvement

TSA has implemented best practices in the execution of its security screening mission to improve overall security effectiveness and operational efficiency as defined in the GFI provided as part of this contract. The Offeror is encouraged to adopt one or more, or a combination, of these best practices in the performance of the contract. TSA may request the Offeror to participate, as a negotiated task order modification, in short-term airport pilot initiatives that adds to airport security screening services effectiveness. Additionally, the Offeror shall regularly assess screening operations and collaborate with TSA to propose and implement improvements. The Offeror is encouraged to propose and implement innovative and modernization solutions at the checkpoint and other applicable locations, subject to TSA approval.

1.7 Transition

This section defines the Offeror's responsibilities to Transition into and out of the IDIQ and subsequent orders to enable continuity of operations at Gold+ airports.

1.7.1 Performance Requirements

The Offeror shall provide transition support that meets or exceeds the performance requirements in this section.

1.7.1.1 Transition In

The Offeror shall provide a full suite of services to transition into the IDIQ and subsequent orders. This includes, but not limited to, vetting activities, transferring Government Furnished Equipment (GFE) / Government Furnished Information (GFI), obtaining PIV badges, and meetings. The Offeror shall submit a Transition Plan (if applicable) outlining transition in and transition out activities as well as weekly Transition Reports until activities have been completed. The Transition Plan shall be updated as appropriate throughout the life of the contract.

In connection with conducting the transition, the Offeror shall report its compliance with FAR Clause 52.207-3 Right of First Refusal of Employment (May 2006).

1.7.1.2 Transition Out

The Offeror shall provide the full suite of services to transition out of the IDIQ. This includes, but not limited to, four months of services migration (unless directed otherwise) of contractual responsibilities from the Offeror's supervision to another Offeror or to TSA. Government owned

equipment and property shall be transferred to TSA or as otherwise directed by TSA. Offeror-owned or leased equipment and property shall be removed from the site by the Offeror at the end of the contract or as otherwise directed by TSA, ensuring that removal does not disrupt ongoing operations or transition activities. The Offeror shall coordinate all removal activities with TSA and ensure that any such removal is completed in a safe and timely manner, in accordance with TSA security and safety requirements. The Offeror shall provide TSA with a detailed inventory of all Offeror-owned equipment and property on an annual basis, at least 60 days prior to base year/option year end and contract end. Any equipment or property that the Offeror proposes to leave in place or transfer to TSA or the incoming Offeror must be approved in writing by TSA. The Offeror shall transfer all data and records to TSA and dispose of items as appropriate.

To ensure continuity of operations in the event of financial distress, default, or other circumstances requiring rapid transition back to TSA, the Offeror shall demonstrate a financial mechanism, as approved by TSA, sufficient to fund continued screening services for a minimum of 180-days. This mechanism shall cover operational costs during the transition period until TSA, or a successor provider can assume full responsibility. The Offeror shall provide evidence of this account and update TSA on its status as part of regular contract administration. An escrow account, Irrevocable Letter of Credit (ILOC), Performance Bond, or Corporate Guarantee are acceptable mechanisms to satisfy the 180-day financial security requirement.

Upon commencement of the transition out phase, the Offeror shall update the Transition Plan in collaboration with TSA and submit weekly Transition Reports until activities have been completed.

1.8 Travel and Other Direct Costs

All cost-reimbursable travel and Other Direct Costs (ODC) shall be approved in advance by the COR and specified in the task order. ODCs may include, but are not limited to, travel, lodging, per diem, shipping, materials, supplies, equipment rental, and other expenses directly attributable to contract performance and not included in the Offeror's indirect rates. All travel shall be conducted in accordance with the Federal Travel Regulations (FTR) and applicable contract clauses. All ODCs must be reasonable, allocable, allowable, and supported by appropriate documentation. The Offeror shall submit requests for reimbursement of travel and ODCs in accordance with the procedures and formats specified by TSA.

2 Deliverables

Work products and deliverables required as part of the scope under this IDIQ and shall be submitted in draft and final form to the Government during the actual task order execution. No proprietary tools, software, or applications shall be required to open or view deliverables unless approved by the CO or COR. Draft due dates provide the opportunity for an initial review of the work product to ensure it aligns with the Governments desired format, types of information, and level of detail. All deliverables are to be submitted to the COR unless otherwise specified by the Government.

TSA has provided templates for some of the deliverables listed below. The Offeror shall use provided templates or proposed by the Offeror, subject to TSA approval, as specified.

Item	Title	Frequency	Final Due Date	Format / Template
1	Kickoff Meeting	As needed	1 business day prior to kickoff meeting	Offeror proposed format
2	Transition In Plan	As needed	15 business days after kickoff	Offeror proposed format
3	Transition Report	Weekly	5 business days after award; weekly until transition is complete	Offeror proposed format
4	Contract Status Report (CSR)	Monthly	10 business days after last business day of the month	Offeror proposed format
5	Program Management Review (PMR)	Quarterly	1 business day prior to PMR meeting	Offeror proposed format
6	Operations Management Plan (OMP)	As needed	15 business days after kickoff	Offeror proposed format
7	Financial Report	Annual	30 days after fiscal year end	Offeror proposed format
8	Reinvestment Analysis	Annual	30 days after fiscal year end	Offeror proposed format
9	Quarterly Financial Report	Quarterly	15 days after quarter end	Offeror proposed format
10	Risk Management Plan (RMP)	As needed	15 business days after kickoff	Offeror proposed format; May be combined with OMP
11	Quality Control Plan (QCP)	As needed	15 business days after kickoff	Offeror proposed format; May be combined with OMP
12	Site Design and Installation Plans	As needed	30 days after award	Offeror proposed format
13	As-Built Designs	As needed	30 days after site upgrades and installation	Offeror proposed format
14	Configuration Status Accounting Reports	Monthly	10 business days after last business day of the month	Offeror proposed format
15	Acceptance Testing Report	As needed	15 days after acceptance testing completion	Offeror proposed format
16	Equipment Inventory & RMA Report	Monthly	10 business days after last business day of the month	Offeror proposed format
17	Maintenance Report	Monthly	10 business days after last business day of the month	Offeror proposed format

18	Customer Service Log & Effectiveness Report	Monthly	10 business days after last business day of the month	Offeror proposed format
19	Continuity of Operations (COOP) Plan	As needed	15 business days after kickoff	Offeror proposed format; May be combined with OMP
20	Incident Log	Monthly	10 business days after last business day of the month	Offeror proposed format
21	Staffing/Training Compliance Report	Monthly	10 business days after last business day of the month	Offeror proposed format
22	Claims Management Plan (CMP)	As needed	15 business days after kickoff	Offeror proposed format
23	Image Threat Detection Reports	As needed	3 business day from the request	May be combined with OMP
24	FDRS Reports to include False Alarm Rate and Threat Detection Algorithm version number.	Daily - Per Lane	15 business days after kickoff	FDRS Format or integration with TSA approved systems
25	Performance Metrics Report	As specified for each metric	1 business day after Transition	Offeror proposed format - or integration with TSA approved systems
26	Compliance Metrics Report	As specified for each metric	1 business day after Transition	Offeror proposed format - or integration with TSA approved systems
27	Data Points Report	As specified for each data point	1 business day after Transition	Offeror proposed format - or integration with TSA approved systems

3 Performance Requirements Summary

The Offeror service requirements are summarized into performance objectives, thresholds, and surveillance methods aligned to the contract requirements. The performance objectives are designed to maintain a level of security screening services under the contract that are equal to or greater than the level that would be provided by the Federal Government. The Government will use multiple processes and techniques to monitor and assess Offeror performance over the life of the contract.

Due to the dynamic nature of TSA's mission, performance objectives may change rapidly in advance of contract modifications. TSA reserves the right to review applicable performance objectives and expects the Offeror will respond promptly to TSA requests for improvements.

Specific numeric thresholds for each metric (e.g., [TSA standard], [TSA baseline]) are considered SSI and are based on TSA standards, historical performance, and risk posture. Some baselines will be determined at the time of transition, as they are airport-specific and reflect local conditions. TSA may adjust these thresholds over time to reflect changes in threat, technology, or operational requirements. (See Attachment - Gold+ Performance Metrics)

Performance Metric	**Acceptable Quality Level (AQL)**	**Frequency of Reporting**
Security and Threat Detection		
Threat Detection Rate	≥ [TSA detection standard]	Daily
	≥ [TSA rate]	Daily
Selectee Find Rate	≥ [TSA standard]	Daily
Access Control per 100K Passengers	≥ [TSA detection standard]	Daily
Ensure random unpredictable screening and mitigate insider threats	ATLAS utilization rate ≥ [TSA standard]; ATLAS Weighted Effectiveness ≥ [TSA standard]	Daily
	USP rate ≥ [TSA approved rate]	Daily
Screening Workforce Performance		
Overt test pass rate	≥ [TSA baseline]	Annually
Covert test pass rate	≥ [TSA baseline]	Annually
Field Evaluation pass rate	≥ [TSA standard]	Quarterly
Officers demonstrate Command Presence	≥ [TSA standard]	Daily
Officer image interpretation	≥ [TSA standard]	Monthly
Incident Report Time	≤ [TSA baseline]	Daily
Supervisory Engagement	≥ [TSA baseline]	Daily
Screening Workforce Professionalism	≥ [TSA baseline]	Daily
Checkpoint Management		
Standard lanes: Wait time < 30 minutes	Frequency ≥ [TSA standard] A tiered approach will be applied with % of Total Passengers Screened thresholds	Twice Hourly/Real-time
TSA PreCheck lanes: Wait time <10 minutes	Frequency ≥ [TSA standard] A tiered approach will be applied with % of Total Passengers Screened thresholds	Twice Hourly/Real-time
Operational availability (Ao)	≥ [TSA standard]	Daily
Customer Service		
Trust In TSA Score	≥ [TSA Target]	Monthly
Complaint Trend Score	≤ [TSA baseline]	Monthly
Compliment Trend Score	≥ [TSA baseline]	Monthly

Annual Customer Satisfaction Score (CSAT)	≥ [TSA Target]	Annually
Rate of claims resolved within 60 days	≥ [TSA rate]	Monthly
Innovation & Continuous Improvement		
Tech/process improvements or innovations implemented (as a pilot or full scale)	≥ [Number and timing of improvements /innovations submitted in the proposal and committed to in the contract]	Monthly

3.2. Financial incentives

The following financial incentives apply if Offeror does exceed the monthly acceptable level for the eight metrics as specified in the contract, while meeting the baseline/target across all performance metrics. This incentive structure is designed to drive excellence in security, efficiency, and customer service, while also fostering strong leadership, professionalism, and a positive workforce culture—recognizing that these attributes are essential to long-term mission success. All incentives will be paid only to the extent that the total contract value, including incentives, does not exceed the contractual ceiling established by TSA.

- If any four or more of the eight listed metrics are exceeded for a single month—including at least one security/efficiency metric and one workforce/professionalism metric—the Offeror will receive 5% more than the total monthly invoice value for that period.
- If any six or more of the eight listed metrics are exceeded for a single month, then the Offeror will receive 10% more of the total monthly invoice value for that period.

Monthly Metrics: *Security/Efficiency:* Officer image interpretation; Standard Lanes; Wait time < 10 minutes; PreCheck Lanes: Wait time < 5 minutes; Operational availability (Ao); and *Leadership/Professionalism/Customer Service:* Officers demonstrate Command Presence; Supervisory Engagement; Screening Workforce Professionalism; Trust In TSA Score. (See 33 TSA-RTWT-Requirements_Final_2026-04-27)

If the Offeror exceeded the two annual metrics below, the Offeror would receive 2% of the contract annual value as part of the last invoice paid.
Annual Metrics: Annual Customer Satisfaction Score (CSAT), Number of improvements or innovations implemented (as a pilot or full scale)

The percentage adjustments described above represent maximum monthly (or annual) incentives and are not additive beyond the contract value threshold. In no event will total payments, including incentives, exceed the contract ceiling.

TSA will periodically review and refine the incentive metrics to ensure they are effectively driving the desired behaviors and outcomes and may adjust the structure as needed based on operational experience and industry feedback.

3.3. Financial Disincentives

The following financial disincentives apply if Offeror does not meet the monthly acceptable level for the ten metrics:

- If any two of the ten listed metrics are not met for a single month, then Offeror will credit TSA 2% of total monthly invoice value for that period.

- If any four or more of the ten listed metrics are not met for a single month, then Offeror will credit TSA 4% of the total monthly invoice value for that period.

- If any six or more of the ten listed metrics are not met for a single month, then the Offeror will credit TSA 6% of the total monthly invoice for that period.

Monthly Metrics: Threat detection rate, Selectee Find Rate, Access Control per 100K Passengers, Ensure random unpredictable screening and mitigate insider threats, Officers demonstrate Command Presence, Officer image interpretation, Standard lanes: Wait time < 30 minutes, PreCheck lanes: Wait time <10 minutes, Operational availability (Ao), Incident Report Time.

4 Attachments

- Attachment A - Gold+_CM Req_Attachment_4.13.26
- Attachment B - Gold+_Maintenance Req_Attachment_4.13.26
- Attachment F - checkpoint-requirements-and-planning-guide
- Attachment I - Governance
- Attachment J - SPP
- 18 Attachment C - SSI Policies and Procedures Handbook
- 19 Attachment D - ITAR_Terms-Conditions GOLD+
- 20.1 Attachment E - cap_acceptable_capability_list
- 24 Attachment G - TSA T&E Guidebook Rev 6 - Final
- 25 Attachment H - TSA Handbook 1100.73-2, FINAL, 201218
- 26 Final DRAFT Evaluation Factors - Gold+ 05072026 (003)
- 33 TSA-RTWT-Requirements_Final_2026-04-27
- Gold+ Performance Metrics 04132026