PERFORMANCE WORK STATEMENT (PWS)

FOR

Purchase Wall and Desktop Secure Capable Video

Teleconferencing equip

1.0 General:

1.1 Scope: The contractor shall provide all personnel, equipment, tools, materials, supervision, and quality control necessary, except as specified in Paragraph 3.0 as Government Furnished, to perform ***the install of S-VTC Wall and Desktop mounted equipment, to include verification testing*** as defined in this PWS.

1.1.1 Objectives: 134 ARW at McGhee Tyson ANGB Tn is wanting new Secure capable wall mounted Video Teleconference (S-VTC) equipment and desktop mounted VTC equipment. The current state of both wall and desktop mounted VTC equipment is out dated and often times inoperable when needed for a conference. As with all IT based equipment it must be refreshed ever so often because of industry upgrades and cyber challenges that continually attack networks. With new missions coming on line, it is imperative that this equipment get upgraded to meet the new mission needs. We have market research documents for 3 different options for VTC equipment. All equipment must be TAA and TEMPEST guidance AFSSI-7702 certified including crypto equipment and usable inside SCIF'd facilities.

1.2 Background: This equipment is needed for secure VTC's that cover mission needs for the 134 ARW and 119th COS. Due to new mission requirements this equipment will enhance the Wing's and Squadron's preparedness securing the ability to have face to face meetings in a classified and unclassified environment. The current state of VTC equipment is poor and the technology needs to be completely updated due to current equipment being end of life and not supported any further.

1.3 Period of Performance (PoP): The Period of Performance shall be decided after vendor is selected and equipment can be delivered for installation.

1.4 General Information:

1.4.1 Place and Performance of Services: 0700-1630 Monday – Friday The contractor shall provide warranty services on new equipment 24 hours a day, 7 days a week, except on recognized US holidays or when the Government facility/installation is closed due to local or national emergencies, administrative closings, or similar Government-directed facility/installation closings. Performance shall be at _Building 132 & 134 & 193. The contractor shall at all times maintain an adequate work force for the uninterrupted performance of all tasks defined within this PWS when the Government

facility/installation is not closed for the above reasons. When hiring personnel, the contractor shall keep in mind that the stability and continuity of the work force are essential.

1.4.1.1 Telework: Teleworking is not authorized.

1.4.1.2 Unscheduled gate closures by the Security Police may occur at any time causing all personnel entering or exiting a closed installation to experience a delay. This cannot be predicted or prevented. Contractors are not compensated for unexpected closures or delays. Vehicles operated by contractor personnel are subject to search pursuant to applicable regulations. Any moving violation of any applicable motor vehicle regulation may result in the termination of the contractor employee's installation driving privileges.

1.4.1.3 The contractor's employees shall become familiar with and obey the regulations of the installation; including fire, traffic, safety and security regulations while on the installation. Contractor employees should only enter restricted areas when required to do so and only upon prior approval. All contractor employees shall carry proper identification with them at all times, and shall be subject to such checks as may be deemed necessary. The contractor shall ensure compliance with all regulations and orders of the installation, which may affect performance. The Government reserves the right to direct the removal of an employee from Government property or revoke access to Government systems for misconduct, security reasons, or any overt evidence of communicable disease. Removal of contractor employees for reasons stated above does not relieve the Contractor from responsibility for total performance of this contract.

1.4.2 Recognized Holidays: The following are recognized United States (US) holidays. The contractor ***shall not*** perform services on these days:

1.4.2.1 New Year's Day: January 1st
1.4.2.2 Martin Luther King, Jr.'s Birthday
1.4.2.3 President's Day
1.4.2.4 Memorial Day
1.4.2.5 Juneteenth National Independence Day: June 19th
1.4.2.6 Independence Day: July 4th
1.4.2.7 Labor Day
1.4.2.8 Columbus Day
1.4.2.9 Veteran's Day: November 11th
1.4.2.10 Thanksgiving Day
1.4.2.11 Christmas Day: December 25th

1.4.3 Quality Control (QC):

1.4.4 Quality Assurance (QA): The Government will evaluate the contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan (QASP). This plan is primarily focused on what the Government will do to ensure

that the contractor has performed in accordance with the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and acceptable quality level(s) or defect rate(s). ISSM will ensure all TEMPEST guidelines are met.

1.4.5 Access and General Protection/Security Policy and Procedures. The contractor shall comply with all applicable installation/facility access and local security policies and procedures, which may be obtained from the Contracting Officer's Representative (COR). The contractor shall also provide all information required for background checks to meet installation access requirements to be accomplished by the local installation's Security Forces, Director of Emergency Services or local Security Office. The contractor shall ensure compliance with all personal identity verification requirements as directed by DoD, Headquarters Air Force (HAF) and/or local policy. Should the Force Protection Condition (FPCON) change, the Government may require changes in contractor security matters or processes.

1. The contractor shall obtain base identification and vehicle passes, if required, for all contractor personnel who make frequent visits to or perform work on the Air Force installation(s) cited in the contract. Contractor personnel are required to wear or prominently display installation identification badges or contractor-furnished, contractor identification badges while visiting or performing work on the installation.

2. The contractor shall submit a written request on company letterhead to the contracting officer listing the following: contract number, location of work site, start and stop dates, and names of employees and subcontractor employees needing access to the base. The letter will also specify the individual(s) authorized to sign for a request for base identification credentials or vehicle passes. The contracting officer will endorse the request and forward it to the issuing base pass and registration office or Security Forces for processing. When reporting to the registration office, the authorized contractor individual(s) should provide a valid driver s license, current vehicle registration, valid vehicle insurance certificate, and [insert any additional requirements to comply with local security procedures] to obtain a vehicle pass.

3. During performance of the contract, the contractor shall be responsible for obtaining required identification for newly assigned personnel and for prompt return of credentials and vehicle passes for any employee who no longer requires access to the work site.

4. When work under this contract requires unescorted entry to controlled or restricted areas, the contractor shall comply with ***N/A***

5. Upon completion or termination of the contract or expiration of the identification passes, the prime contractor shall ensure that all base identification passes issued to employees and subcontractor employees are returned to the issuing office.

6. Failure to comply with these requirements may result in withholding of final payment.

1.4.5.1. ***Reserved***

1.4.5.2 Reserved

1.4.5.3 Reserved

1.4.5.4 Reserved.

1.4.5.5 Communications Security/Information Technology (COMSEC/IT) Security. All communications with DoD organizations are subject to COMSEC review. All telephone communications networks are continually subject to intercept by unfriendly intelligence organizations. DoD has authorized the military departments to conduct COMSEC monitoring and recording of telephone calls originating from, or terminating at, DoD organizations. Therefore, the contractor is advised that any time contractor personnel place or receive a call they are subject to COMSEC procedures. The contractor shall ensure wide and frequent dissemination of the above information to all employees dealing with DoD information. The contractor shall abide by all Government regulations concerning the authorized use of the Government's computer network, including the restriction against using the network to recruit Government personnel or advertise job openings.

1.4.5.6 Use of Government Information Systems (IS) and access to Government networks is a revocable privilege, not a right. Users are the foundation of the DoD strategy and their actions affect the most vulnerable portion of the Air Force Infostructure. Contractor employees shall have a favorable background investigation or hold a security clearance and access approvals commensurate with the level of information processed or available on the system. Contractor employees shall:

1.4.5.6.1 Comply with the command's Acceptable Use Policy (AUP) for Government owned IS and sign an AUP prior to or upon account activation.

1.4.5.6.3 Mark and safeguard files, output products, and storage media per classification level and disseminate them only to individuals authorized to receive them with a valid need to know.

1.4.5.6.4 Protect IS and IS peripherals located in their respective areas in accordance with physical security and data protection requirements.

1.4.5.6.5 Practice safe network and Internet operating principles and take no actions that threaten the integrity of the system or network.

1.4.5.7 Reserved

1.4.5.8 Reserved

1.4.5.9 Reserved

1.4.5.10 Reserved

1.4.5.11 Reserved

1.4.5.12 Reserved

1.4.5.13 ***Reserved***

1.4.5.14 Reserved

1.4.6 Physical Security.
The contractor shall safeguard all Government property provided for contractor use. At the close of each work period, Government facilities, equipment and materials shall be secured.

1.4.7 Reserved

1.4.8 Post Award Conference/Periodic Progress Meetings: The contractor agrees to attend any post award conference convened by the KO in accordance with FAR 42.5. The KO, COR and other Government personnel, as appropriate, may meet periodically with the contractor to review the contactor's performance. At these meetings, the KO will apprise the contractor of how the Government views the contractor's performance and the contractor shall apprise the Government of problems, if any, being experienced. The contractor shall resolve outstanding issues raised by the Government. Contractor attendance at these meetings shall be at no additional cost to the Government.

1.4.9 Contract Manager (CM): The contactor shall designate a CM who shall ensure performance under this contract. The name of this person, and an alternate who shall act for the contractor when the CM is absent, shall be designated in writing to the KO. The CM or alternate shall have full authority to act for the contractor on all contract matters relating to daily operation of this contract. The CM shall work through the COR ***(if no COR is assigned, delete through the COR and replace with through the KO)***, to resolve issues, receive technical instructions, and ensure adequate performance of services. The CM shall ensure that contractor employees do not perform any services outside the scope of the contract without an official modification issued by the KO. The CM shall ensure contractor employees understand that services performed outside the scope of the contract are performed wholly at the expense of the contractor.

1.4.10 Reserved

1.4.11. Combating Trafficking in Persons: The United States Government has adopted a zero tolerance policy regarding trafficking in persons. Contractors and contractor employees shall not engage in severe forms of trafficking in persons during the period of performance of the contract; procure commercial sex acts during the period of

performance of the contract; or use forced labor in the performance of the contract. The Contractor shall notify its employees of the United States Government's zero tolerance policy, the actions that will be taken against employees for violations of this policy. The contractor shall take appropriate action, up to and including termination, against employees or subcontractors that violate the US Government policy as described at FAR 22.17.

1.4.12 Reserved

1.4.13 Data Rights
The Government has unlimited rights to all documents/materials produced under this contract. All documents and materials, to include the source codes of any software, produced under this contract shall be Government owned and are the property of the Government with all rights and privileges of ownership/copyright belonging exclusively to the Government. These documents and materials may not be used or sold by the contractor without written permission from the KO. All materials supplied to the Government shall be the sole property of the Government and may not be used for any other purpose. This right does not abrogate any other Government rights.

1.4.14 Organizational Conflicts of Interest (OCI): The contractor and subcontractor personnel performing services under this contract may receive, have access to or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.) or perform evaluation services which may create a current or subsequent OCIs, as defined in FAR Subpart 9.5. The contractor shall notify the KO immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the KO to avoid or mitigate any such OCI. The contractor's mitigation plan will be determined to be acceptable solely at the discretion of the KO. In the event the KO unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the KO may impose other remedies as he or she deems necessary, including prohibiting the contractor from participation in subsequent contracted requirements which may be affected by the OCI.

1.4.15 Reserved

2.0 Definitions and Acronyms:

2.1 Definitions:

2.1.1 Contractor: A supplier or vendor awarded a contract to provide specific supplies or service to the Government. The term used in this contract refers to the prime.

2.1.2 Defective Service: A service output that does not meet the standard of performance associated with the PWS.

2.1.3 Deliverable: Anything that can be physically delivered and includes non-manufactured things such as meeting minutes or reports.

2.1.4 Key Personnel: Contractor personnel that are evaluated in a source selection process and that may be required to be used in the performance of a contract by the PWS. When key personnel are used as an evaluation factor in best value procurement, an offer can be rejected if it does not have a firm commitment from the persons that are listed in the proposal.

2.1.5 Physical Security: Actions that prevent the loss or damage of Government property.

2.1.6 Quality Assurance: The Government procedures to verify that services being performed by the Contractor are performed according to acceptable standards.

2.1.7 Quality Assurance Surveillance Plan (QASP): An organized written document specifying the surveillance methodology to be used for surveillance of contractor performance.

2.1.8 Quality Control: All necessary measures taken by the Contractor to ensure that the quality of an end product or service shall meet contract requirements.

2.1.9 Subcontractor: One that enters into a contract with a prime contractor. The Government does not have privity of contract with the subcontractor.

2.2 Acronyms:

AEI	Army Enterprise Infostructure
AR	Army Regulation
AT/OPSEC	Antiterrorism/Operational Security
BI	Background Investigation
CM	Contract Manager
COR	Contracting Officer Representative
DA	Department of the Army
DD254	Department of Defense Contract Security Classification Specification
DFARS	Defense Federal Acquisition Regulation Supplement
DoD	Department of Defense
DSCA	Defense Counterintelligence and Security Agency
FAR	Federal Acquisition Regulation
GFP/M/E/S	Government Furnished Property/Material/Equipment/Services
HQDA	Headquarters, Department of the Army
HSPD	Homeland Security Presidential Directive
IA	Information Assurance
IS	Information System(s)
KO	Contracting Officer
NGB	National Guard Bureau

OCI	Organizational Conflict of Interest
PII	Personally Identifiable Information
PIPO	Phase In/Phase Out
POC	Point of Contact
PRS	Performance Requirements Summary
PWS	Performance Work Statement
QA	Quality Assurance
QASP	Quality Assurance Surveillance Plan
QC	Quality Control
QCP	Quality Control Program
SCR	Service Contract Reporting
SSN	Social Security Number
TE	Technical Exhibit
USD(I)	Under Secretary of Defense for Intelligence

3.0 Government Furnished Property, Material, Equipment and Services (GFP/M/E/S): The Government will provide the property, material, equipment, and/or services listed below solely for the purpose of performance under this contract:

3.1 Property: The Government will furnish the necessary workspace for the contractor to perform services outlined in this PWS to include desk space, telephones, computers and other items necessary to maintain an office environment.

3.2 Materials: ***Desk Space***

3.3 Reserved

3.4 Reserved

3.5 Utilities: All utilities in the facility will be available for the contactor's use in the performance of this contract. The contractor shall instruct employees in utilities conservation practices. The contractor shall operate under conditions that preclude the waste of utilities, which include turning off the water faucets or valves after using the required amount.

4.0 Contractor Furnished Property, Materials, and Equipment (CFP/M/E):

TSG and TEMPEST Video Teleconferencing Room Bar with Navigator TAA or equivalent.

TSG desktop VTC with power injectors and TAA complaint.

US PS 8X5XNBD CS-BAR-K9 or equivalent.

DM Essentials 4K60 4:4:4 Receiver for HDMI, Fiber, and IR Signal Extension over 1G LC Fiber Cable following TEMPEST (AFSSI-7702) requirements or equivalent.

DM Essentials 4K60 4:4:4 Transmitter for HDMI, fiber, and IR Signal Extension over Fiber Cable following TEMPEST requirements or equivalent.

DM Essentials 4K60 4:4:4 Transmitter for USB-C DisplayPort, USB 2.0, and Ethernet Signal Extension over Fiber Cable following TEMPEST requirements or equivalent.

DM Essentials 4K60 4:4:4 Receiver for HDMI, USB 2.0, and Ethernet Signal Extension over CATx and or Fiber Cable following TEMPEST requirements or equivalent.

2x1 8K AV Switcher and Smart Display Controller w/ 2 LC Fiber video output ports, FO audio output port, FO Content in Port, Ext. MicPod port or equivalent.

Matching Microphone Array for table and Web w/TSG positive disconnect or equivalent.

5-Port Gigabit PoE++ Powered Managed Switch with PoE Passthrough or equivalent.

Gigabit POE+ Injector 30 Watt or equivalent.

TAA Compliant** 65" Commercial Display, UHD (3840x2160), 500cd/m2

FIXED, HEIGHT ADJ., STATIC MOUNT, TAA

Complete installation and verification testing.

4.1 General: Except for those items specifically stated to be Government-Furnished in Paragraph 3.0, the contractor shall furnish everything required to perform these services as indicated in Paragraph 1.1.

4.2 Reserved

4.3 Reserved

5.0 Requirements: The contractor shall: Supply and install new Secure (Top Secret/Secret) capable Video Teleconference (S-VTC) wall and/or desktop mounted packages. This requirement has different options available depending on funding avenues, this project could increase to a total of 12 complete set-ups. Meeting all

TEMPEST and secure Internet rules and regulations to include both TSG and TEMPEST standards.

5.1 CLIN #1 FUNDED: WOC 1 S-VTC: 134 ARW at McGhee Tyson ANGB TN requires new Secure capable wall mounted Video Teleconference (S-VTC) equipment. New S-VTC equipment must be TSG and TEMPEST certified with 65" wall mounted Display. The TSG-approved and TEMPEST-certified VTC w / 65" Display Bundle your installation must prioritize physical-layer separation, secure optical path integrity, and positive disconnect functionality inspections. Installation team must verify that the installer has strictly separated all red/black signals, correctly terminated the fiber optic (FO) runs, and validated the hardwired TSG positive disconnect mechanisms. Install team must ensure cable separation, power filtering and fiber cleaning and document test results. When the system is muted or idle, there must be a clear, unambiguous physical indicator showing that the microphones are disconnected. Installers will ensure all wireless/transmitting components (such as Wi-Fi and Bluetooth antennas/chips) have disabled or physically removed from S-VTC equipment. Rack space and wall space will be made available for install team.

CLIN #2 119th FUNDED: This requirement is for equipment only, purchaser will install in secure areas. Need is 3 - TSG-A Cisco WebEx Desk Class A with Power Injector VTC to replace current End of Service, operational risk of loosing critical capability. Desktop VTCs must be TAA Compliant in order to connect to JWICS. Additionally, this is the only known VTC that works with SIPR Teams Meeting. Current Desktop VTC equipment is End of Service and no longer supported. This highly specialized equipment must have tamper evident labels, capability to secure chassis to desktop and has integrated privacy shutter that physically blocks the lens. Must ensure installers use shielded twisted pair Cat6/6A cabling with metal bonded RJ-45 connectors.

CLIN #3 HQ's UNFUNDED: 2 S-VTC; 134 ARW at McGhee Tyson ANGB TN requires new Secure capable wall mounted Video Teleconference (S-VTC) equipment. New S-VTC equipment must be TSG and TEMPEST certified with 65" wall mounted Display. The TSG-approved and TEMPEST-certified VTC w / 65" Display Bundle your installation must prioritize physical-layer separation, secure optical path integrity, and positive disconnect functionality inspections. Installation team must verify that the installer has strictly separated all red/black signals, correctly terminated the fiber optic (FO) runs, and validated the hardwired TSG positive disconnect mechanisms. Install team must ensure cable separation, power filtering and fiber cleaning and document test results. When the system is muted or idle, there must be a clear, unambiguous physical indicator showing that the microphones are disconnected. Installers will ensure all wireless/transmitting components (such as Wi-Fi and Bluetooth antennas/chips) have disabled or physically removed from S-VTC equipment. Rack space and wall space will be made available for install team.

CLIN #4 134 MXG UNFUNDED: 1 S-VTC; 134 ARW at McGhee Tyson ANGB Tn requires new Secure capable wall mounted Video Teleconference (S-VTC) equipment. New S-VTC equipment must be TSG and TEMPEST certified with 65" wall mounted Display. The TSG-approved and TEMPEST-certified VTC w / 65" Display Bundle your installation must prioritize physical-layer separation, secure optical path integrity, and positive disconnect functionality inspections. Installation team must verify that the installer has strictly separated all red/black signals, correctly terminated the fiber optic (FO) runs, and validated the hardwired TSG positive disconnect mechanisms. Install team must ensure cable separation, power filtering and fiber cleaning and document test results. When the system is muted or idle, there must be a clear, unambiguous physical indicator showing that the microphones are disconnected. Installers will ensure all wireless/transmitting components (such as Wi-Fi and Bluetooth antennas/chips) have disabled or physically removed from S-VTC equipment. Rack space and wall space will be made available for install team.

CLIN #5 119th UNFUNDED 4-Desktop CISCO Webex: This requirement is for equipment only, purchaser will install in secure areas. Need is 4 - TSG-A Cisco WebEx Desk Class A with Power Injector VTC to replace current End of Service, operational risk of loosing critical capability. Desktop VTCs must be TAA Compliant in order to connect to JWICS. Additionally, this is the only known VTC that works with SIPR Teams Meeting. Current Desktop VTC equipment is End of Service and no longer supported. This highly specialized equipment must have tamper evident labels, capability to secure chassis to desktop and has integrated privacy shutter that physically blocks the lens. Must ensure installers use shielded twisted pair Cat6/6A cabling with metal bonded RJ-45 connectors.

CLIN #6 119th UNFUNDED 6-S-VTC; 119th COS at McGhee Tyson ANGB Tn requires new Secure capable wall mounted Video Teleconference (S-VTC) equipment. New S-VTC equipment must be TSG and TEMPEST certified with 65" wall mounted Display. The TSG-approved and TEMPEST-certified VTC w / 65" Display Bundle your installation must prioritize physical-layer separation, secure optical path integrity, and positive disconnect functionality inspections. Installation team must verify that the installer has strictly separated all red/black signals, correctly terminated the fiber optic (FO) runs, and validated the hardwired TSG positive disconnect mechanisms. Install team must ensure cable separation, power filtering and fiber cleaning and document test results. When the system is muted or idle, there must be a clear, unambiguous physical indicator showing that the microphones are disconnected. Installers will ensure all wireless/transmitting components (such as Wi-Fi and Bluetooth antennas/chips) have disabled or physically removed from S-VTC equipment. Rack space and wall space will be made available for install team.

5.2 Justifications:

5.3 Justifications: •

6.0 Applicable Publications: Publications applicable to this PWS are listed below:

Publication (Chapter/Page)	Date of Publication	Mandatory or Advisory	Website
Federal Acquisition Regulation			https://www.acquisition.gov/?q=browsefar
Defense Federal Acquisition Regulation Supplement			http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html or https://www.acquisition.gov/dfars
Joint Travel Regulation (JTR)			https://www.defensetravel.dod.mil/site/travelreg.cfm
DoDM 1000.13-M-V1 DoD Identification (ID) Cards (Enclosure 2, paragraph 3.b)	01/23/2014 (Change 1: 07/28/2020)		http://www.esd.whs.mil/Directives/issuances/dodm
Federal Information Processing Standards (FIPS) Publication 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors (paragraph 9)	August 2013		http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf
DoDM 5200.2 Procedures for the DoD Personnel Security Program (PSP)	04/03/2017		https://www.esd.whs.mil/Directives/issuances/dodm/
DoDI 5200.46 DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC)	09/09/14 (Change 1: 05/04/2018)		https://www.esd.whs.mil/Directives/issuances/dodi/
Homeland Security Presidential Directive (HSPD)-12 Policy for a Common Identification Standard for Federal Employees and Contractors	08/27/2004		https://www.dhs.gov/homeland-security-presidential-directive-12
DoDI 5400.11 Department of Defense Privacy and Civil Liberties Programs	01/29/2019		https://www.esd.whs.mil/Directives/issuances/dodi/
DoD 5400.11-R Department of Defense Privacy Program	05/14/2007		https://www.esd.whs.mil/Directives/issuances/dodm/
DoDD 8140.01 Cyberspace Workforce Management	10/05/2020		https://www.esd.whs.mil/Directives/issuances/dodd/
DoD 8570.01-M Information Assurance Workforce Improvement Program	12/19/2005 (Change 4: 11/10/2015)		https://www.esd.whs.mil/Directives/issuances/dodm/
DoD 5220.22-M National Industrial Security Program Operating Manual (NISPOM)	02/28/2006 (Change 2: 05/18/2016)		https://www.esd.whs.mil/Directives/issuances/dodm/
Army Directive 2014-05 Policy and Implementation Procedures for Common Access Card Credentialing and Installation Access for Uncleared Contractors	03/07/2014		https://armypubs.army.mil/ProductMaps/PubForm/ArmyDir.aspx
AR 25-2 Information Assurance	04/04/2019		http://armypubs.army.mil/ProductMaps/PubForm/AR.aspx
AR 530-1 Operations Security	09/26/2014		http://armypubs.army.mil/ProductMaps/PubForm/AR.aspx
AR 525-13 Antiterrorism	12/09/2019		http://armypubs.army.mil/ProductMaps/PubForm/AR.aspx
AR 381-12	06/01/2016		http://armypubs.army.mil/ProductMaps/PubForm/AR.aspx

Threat Awareness and Reporting Program (TARP) (Section II, ¶ 2-4.b)			
AFI 10-245 Antiterrorism	03/28/2013 (Certified current 03/30/2017)		https://www.e-publishing.af.mil/Product-Index/#/?view=pubs&orgID=10141&catID=1&series=-1&modID=449&tabID=131
AFI 31-101 Security Forces Standards and Procedures	08/18/2020		https://www.e-publishing.af.mil/Product-Index/#/?view=pubs&orgID=10141&catID=1&series=-1&modID=449&tabID=131
AFMAN 31-113 Security Forces Standards and Procedures	03/05/2013 Change 1: 12/02/2015		https://www.e-publishing.af.mil/Product-Index/#/?view=pubs&orgID=10141&catID=1&series=-1&modID=449&tabID=131
AFPD 17-1 Information Dominance Governance and Management	04/12/2016		https://www.e-publishing.af.mil/Product-Index/#/?view=pubs&orgID=10141&catID=1&series=-1&modID=449&tabID=131
AFMAN 17-1301 Computer Security (COMPUSEC)	02/12/2020		https://www.e-publishing.af.mil/Product-Index/#/?view=pubs&orgID=10141&catID=1&series=-1&modID=449&tabID=131
AFI 10-701 Operations Security	7/24/2019 (Change 1: 06/09/2020)		https://www.e-publishing.af.mil/Product-Index/#/?view=pubs&orgID=10141&catID=1&series=-1&modID=449&tabID=131

6.1 Applicable Forms: Forms applicable to the PWS are listed below:

Form	Date	Website
DD 1172-2 Application for Identification Card/DEERS Enrollment	Mar 2017	http://www.dtic.mil/whs/directives/forms/index.htm
I-9 Employment Eligibility Verification	10/21/2019	https://www.uscis.gov/sites/default/files/files/form/i-9.pdf
DD 441 Department of Defense Security Agreement	Feb 2020	http://www.dtic.mil/whs/directives/forms/dd/ddforms0001-0499.htm
DD 250 Material Inspection and Receiving Report	Aug 2000	https://www.esd.whs.mil/Directives/forms/dd0001_0499/