Preparing Activity: USACE Superseding
UFGS-28 08 10 (May 2016)

UNIFIED FACILITIES GUIDE SPECIFICATIONS

References are in agreement with UMRL dated July 2023
****

SECTION TABLE OF CONTENTS

DIVISION 28 - ELECTRONIC SAFETY AND SECURITY

SECTION 28 08 10

ELECTRONIC SECURITY SYSTEM ACCEPTANCE TESTING

08/23

PART 1 GENERAL

1.1 SUMMARY
1.2 DEFINITIONS
1.3 SUBMITTALS
1.4 QUALITY ASSURANCE
1.4.1 Qualifications
1.4.1.1 General
1.4.1.2 Test Director
1.4.1.3 Operator
1.4.1.4 Technician
1.4.1.5 Test Intruder

PART 2 PRODUCTS

PART 3 EXECUTION

3.1 TEST PLAN
3.1.1 Personnel
3.1.2 Equipment
3.1.3 Procedures
3.1.4 Special Provisions
3.1.5 Test Logs
3.1.6 Schedule
3.2 PRE-ACCEPTANCE TESTING
3.3 SYSTEM ACCEPTANCE
3.3.1 Test Termination Assessment Period
3.3.2 Preparation
3.3.3 Personnel
3.3.4 Visual Inspection
3.3.5 Phased Testing
3.3.5.1 Functional Testing
3.3.5.2 System Activity Reports

3.3.5.3 Corrective Actions
3.3.5.4 Endurance Testing
3.4 FINAL TEST REPORT
3.4.1 Summary
3.4.2 Personnel
3.4.3 Test Logs
3.4.4 False and Nuisance Alarm Rates
3.4.4.1 Valid or Actual Alarm
3.4.4.2 False Alarm
3.4.4.3 Nuisance Alarm
3.4.4.4 Test or Authorized Alarm
3.5 Probability of Detection and Confidence Level

-- End of Section Table of Contents --

****

USACE / NAVFAC / AFCEC / NASA	**UFGS-28 08 10 (August 2023)**

Preparing Activity: USACE	**Superseding** **UFGS-28 08 10 (May 2016)**

UNIFIED FACILITIES GUIDE SPECIFICATIONS

References are in agreement with UMRL dated July 2023

****

SECTION 28 08 10

ELECTRONIC SECURITY SYSTEM ACCEPTANCE TESTING
08/23

****

NOTE: This guide specification covers the requirements for acceptance testing of electronic security systems. An electronic security system includes all equipment, components, control systems, devices, and associated software used to secure facilities and assets through intrusion detection, access control, and video surveillance systems.

Adhere to UFC 1-300-02 Unified Facilities Guide Specifications (UFGS) Format Standard when editing this guide specification or preparing new project specification sections. Edit this guide specification for project specific requirements by adding, deleting, or revising text. For bracketed items, choose applicable item(s) or insert appropriate information.

Remove information and requirements not required in respective project, whether or not brackets are present.

Comments, suggestions and recommended changes for this guide specification are welcome and should be as a Criteria Change Request (CCR)..

****

PART 1 GENERAL

****

NOTE: When this specification is used, it will be in conjunction with UFGS 28 10 05 ELECTRONIC SECURITY SYSTEMS (ESS).

For Air Force projects, use this specification in conjunction with applicable Air Force testing policy and standards.

****

1.1 SUMMARY

This specification defines the process and procedures for initial acceptance testing of electronic security systems (ESS) to include intrusion detection, access control and video as well as associated power and communications. Requirements to plan, conduct, and document all testing activities are covered along with the Government responsibility to witness testing and review and approve submittals. During the course of the acceptance test, demonstrate that, without exception, the completed and integrated ESS complies with the contract requirements.

1.2 DEFINITIONS

The Government Representative is a qualified individual given specific authority to witness system acceptance testing and evaluate the results.

1.3 SUBMITTALS

****

NOTE: Review submittal description (SD) definitions in Section 01 33 00 SUBMITTAL PROCEDURES and edit the following list, and corresponding submittal items in the text, to reflect only the submittals required for the project. The Guide Specification technical editors have classified those items that require Government approval, due to their complexity or criticality, with a "G." Generally, other submittal items can be reviewed by the Contractor's Quality Control System. Only add a “G” to an item, if the submittal is sufficiently important or complex in context of the project.

For Army projects, fill in the empty brackets following the "G" classification, with a code of up to three characters to indicate the approving authority. Codes for Army projects using the Resident Management System (RMS) are: "AE" for Architect-Engineer; "DO" for District Office (Engineering Division or other organization in the District Office); "AO" for Area Office; "RO" for Resident Office; and "PO" for Project Office. Codes following the "G" typically are not used for Navy, Air Force, and NASA projects.

The "S" classification indicates submittals required as proof of compliance for sustainability Guiding Principles Validation or Third Party Certification and as described in Section 01 33 00 SUBMITTAL PROCEDURES.

Choose the first bracketed item for Navy, Air Force and NASA projects, or choose the second bracketed item for Army projects.

****

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are [for Contractor Quality Control approval.][for information only. When used, a code following the "G" classification identifies the office that

will review the submittal for the Government.] Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-05 Design Data

Test Plan; G[, [_____]]

SD-06 Test Reports

Final Test Report; G[, [_____]]

Pre-Acceptance Test Certification; G[, [_____]]

SD-07 Certificates

Qualifications

1.4 QUALITY ASSURANCE

1.4.1 Qualifications

****
NOTE: Adjust years of experience required for the Test Director, Operator, and Technician to reflect the size and complexity of the ESS.

Government personnel may be allowed to participate in the role of Operator.
****

1.4.1.1 General

The Test Director, Operator, and Technician must have prior experience with the specific equipment, hardware and software installed under the contract.

1.4.1.2 Test Director

The Test Director must have at least [five] [_____] years of hands-on ESS experience to include any combination of design, installation, testing and maintenance.

1.4.1.3 Operator

The Operator must have at least [two] [_____] years of hands-on experience installing and maintaining ESS workstations to include both hardware and software. The Operator must be capable of demonstrating all workstation features and capabilities.

1.4.1.4 Technician

The technician must have at least [two] [_____] years of hands-on experience installing and maintaining ESS field equipment to include sensors, card readers, cameras, local processors, and communications equipment. The Technician must be capable of demonstrating all features and capabilities of ESS field equipment. Qualifications may be met by the individual experience of one technician or by the combined experience of a team of technicians.

[1.4.1.5 Test Intruder

****

NOTE: Include the qualifications for a test intruder only if the project includes intrusion sensors that are activated by: 1) an intruder moving through a volumetric or linear detection pattern or 2) an intruder climbing a fence. These sensors include passive infrared, active infrared, microwave, buried ported coaxial cable, and fence-mounted sensors. Insert the allowable height and weight range to match the design basis threat for the project. Be aware of the security classification of the design basis threat. If intruder height and weight are classified, do not include these values in this specification. Provide classified information to the Contractor through authorized channels.

If there is no design basis threat for the project, use the default height and weight range which corresponds to the average height and weight of a 20 - 29 year old male in the host nation where the site is located.

For Army projects, contact the Electronic Security System Mandatory Center of Expertise (ESS MCX) for assistance in determining requirements for the Test Intruder. ESS MCX email address is AskESSMCX@usace.army.mil

****

The purpose of the test intruder is to activate intrusion sensors in a realistic and repeatable manner. The test intruder must be between 1780 to 1830 mm [70] [_____] and [72][____] inches tall and weigh between 80 to 85 kg [175] [____] and [190] [_____] pounds. The test intruder must possess sufficient physical strength, agility, and endurance to perform movements required for intrusion testing. These movements may include, but are not limited to, walking, running, crawling, jumping, and climbing.

]PART 2 PRODUCTS

Not Used

PART 3 EXECUTION

3.1 TEST PLAN

The Government will witness all system acceptance testing and endurance testing. Obtain written permission from the Government before proceeding with testing. Clearly establish the scope for ESS testing prior to beginning testing. Submit a Test Plan that addresses all testing requirements to include the following topics:

3.1.1 Personnel

Identify the Test Director, Operator, Technician, [Test Intruder], and any other personnel that will be performing test activities.

3.1.2 Equipment

List all equipment that is required to support testing. State the purpose of each piece of equipment. Describe equipment that will be used to enable voice communications between the monitoring location and the field.

3.1.3 Procedures

Provide a step-by-step procedure for conducting each functional test. Describe actions and expected results. Ensure that functional test procedures address performance standards described in contract specifications especially any probability of detection (Pd) and nuisance and false alarm rate (NAR/FAR) requirements. Pd and NAR/FAR are not typically a concern for interior sensors installed per manufacturers specifications. For exterior sensors NAR/FAR needs to be verified but Pd may not need to be verified if installed IAW manufacturers or service specific guidance.

****

NOTE: Example ESS functional test procedures may be downloaded from http://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/for **These are intended to aid the Contractor in preparing test plans.**

For Air Force Projects, follow the Electronic Security Equipment (ESE) Master Installation Acceptance Test and Turnover Plan, ESE-TP-0023.

****

Download example procedures from http://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/forms-graphic and review for applicability and completeness. Adapt example procedures to meet specific project requirements and develop additional ones as needed. Follow TEST-MASTERTP0023-005 for Air Force projects.

3.1.4 Special Provisions

Discuss any special test provisions such as facility access, safety, integration with existing systems, and coordination with other work.

3.1.5 Test Logs

Provide logs for recording all data from functional testing and burn-in testing.

****

NOTE: Example ESS test logs may be downloaded from http://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/for **These are intended to aid the Contractor in preparing test plans.**

****

Download example logs from http://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/forms-graphic and review for applicability and completeness. Adapt example logs to identify each component by location to meet specific project components and system test requirements. Develop additional logs as needed.

3.1.6 Schedule

Provide an overall schedule that includes all testing milestones.

3.2 PRE-ACCEPTANCE TESTING

****

NOTE: Perform pre-acceptance based on the sponsoring activity requirements. The contractor must confirm system readiness prior to scheduling the system acceptance test.

****

Conduct a complete test of all field equipment, workstations, and central system hardware and software in accordance with the approved Test Plan. The Test Director must be on site to conduct a pre-test inspection and oversee all testing activities. Prior to testing, visually inspect all ESS components and correct workmanship and neatness deficiencies as needed. During the pre-test inspection, verify the accuracy of redline drawings and update drawings as needed. Verify and document performance of each device and system feature to include sensor nuisance and false alarm rates. Review all positioning and field of view adjustments for each camera view in day and night operation.

Prepare and submit Pre-Acceptance Test Certification detailing the results of the testing. Refer to paragraph FINAL TEST REPORT for required content. Include a cover letter signed by the Test Director stating that pre-acceptance testing has been completed and that the system is ready for acceptance testing.

3.3 SYSTEM ACCEPTANCE

Test the ESS in accordance with the approved Test Plan in the presence of the Government Representative to certify acceptable performance. Verify that the total system meets all requirements of the specification and complies with the specified standards.

a. Demonstrate that the completed system complies with the contract requirements. Using approved test procedures, all physical and functional requirements of the project must be demonstrated and shown. The SAT, as specified, is not to be started until after receipt by the Contractor of written permission from the Government.

b. Begin acceptance testing upon arrival of the Government Representative at the project site. Place the ESS in normal operating mode and evaluate system performance during the testing period. Immediately report any deficiencies observed during testing to the Government Representative and discuss possible causes and corrective measures. Obtain Government approval prior to making any adjustments, repairs or modifications. The Government retains the right to terminate testing at any time the ESS is found to be incomplete or fails to perform as specified. Such termination of acceptance testing constitutes a FAILED system acceptance test.

c. Upon termination of testing by the Government or by the Contractor, commence an assessment period as described in paragraph Test Termination Assessment Period.

d. Upon successful completion of the system acceptance test, deliver test reports and other documentation as specified to the Government prior to commencing the endurance test.

3.3.1 Test Termination Assessment Period

Identify all failures, determine causes of all failures, repair all failures, and deliver a written report to the Government. Ensure that the report explains in detail the nature of each failure, corrective action taken, results of tests performed, and recommend the point at which testing should be resumed. After delivering the written report, convene a test review meeting to present the results and recommendations to the Government. Schedule the test review meeting at least 5 business days after receipt of the report by the Government. As a part of this test review meeting, demonstrate that all failures have been corrected by performing appropriate portions of the system acceptance test. Based on the Contractor's report and the test review meeting, the Government will determine the restart date, or may require that the entire test be repeated.

3.3.2 Preparation

****

NOTE: Adjust the notification requirement as needed to accommodate the scheduling needs of the Government Representative. Consider travel planning if the Government Representative's normal duty location is not the project site. Foreign travel may require several weeks advance notice.

****

Notify the Contracting Officer of system readiness [15] [_____] days prior to the expected start date of acceptance testing. Prior to acceptance testing, complete all clean-up and patch work requirements. Ensure that security equipment closets and similar areas are free of accumulation of waste materials or rubbish caused by prior installation work.

3.3.3 Personnel

Ensure that the following personnel are on site to perform test activities: Test Director, Operator, Technician[, and Test Intruder]. Ensure that the Quality Control Manager is on site during acceptance testing.

3.3.4 Visual Inspection

Assist the Government Representative in conducting a visual inspection of ESS equipment and wiring. This inspection will focus on the general neatness and quality of workmanship and compliance with applicable codes and manufacturers' recommended installation methods. Provide a comprehensive listing of installed equipment and software, sorted by location, along with a complete set of ESS red line drawings to be used during the inspection. Document deficiencies identified during the inspection.

3.3.5 Phased Testing

3.3.5.1 Functional Testing

During the functional testing, verify system performance in accordance with the approved Test Plan. Record results in approved Test Logs and provide a written explanation of each failure to include cause, corrective action, and retest result. Continue functional testing until all tests have been successfully completed with no unresolved failures. Comply with requests from the Government Representative to repeat functional tests performed previously. The Government reserves the right to request the Contractor to repeat all functional tests or a representative sampling thereof as a means of performance verification. Document all test results on approved Test Logs.

3.3.5.2 System Activity Reports

Retrieve archived data from the system and provide unaltered activity reports as requested by the Government Representative. Reports may address any type of activity to include alarms, portal transactions, and video archives. Assist with analyzing reports to identify trends and anomalies.

3.3.5.3 Corrective Actions

Correct any deficiencies in coordination with the Government Representative. Maintain a punch list and review status at the end of each day. Work diligently to complete corrective actions the same day that deficiencies are observed. Add deficiencies not corrected on the same day to the rework items list maintained by the Quality Control Manager. Failure to resolve punch list items to the satisfaction of the Government constitutes a FAILED system acceptance test.

3.3.5.4 Endurance Testing

****

NOTE: Consider the size, technology types, and complexity of the ESS installation project when specifying the duration of endurance testing. Consider a 24-hour burn-in testing duration only for a very simple ESS installation involving no more than 25 discrete components. Consider a burn-in testing duration greater than 120 hours for a project with a large number of IDS zones, especially outdoor perimeter zones for which nuisance and false alarms are a concern. Suggested time frames for endurance testing based on technology type are listed below.

1. Video System (no Analytics/ Artificial Intelligence (AI)): 3 to 5 days

2. Video System with Analytics/AI = 5 to 10 days

3. ACS (small) < 20 readers: 3 to 5 days

4. ACS (large)20 < readers < 100: 5 to 10 days

5. Interior IDS (Small) < 7 intrusion zones: 5 days

6. Exterior IDS sensors (Any size): > 9 days

1)Endurance testing for interior IDS should not be less than 5 days, unless the system is very small based on the number of intrusion zones.

2) Endurance testing for exterior IDS should not be less than 7 days

8. Enterprise IDS/ACS/CCTV = > 9 days

****

Following the successful completion of the functional test and completion of all corrective actions, monitor all components for a continuous period of [24] [72] [120] [_____] hours [5] [7] [10] [_____] days upon written approval from the government representative. Active monitoring will take place for a total of [24 hours per day] [8 hours per day and staggered throughout duty hours to sample normal operational and environmental site conditions during daytime and nighttime hours]. All events, anomalies, and alarms will be reviewed, assessed in real time, and documented. Date and time of each activation will be recorded, assessed for cause, and noted. [Events that occur outside the 8-hour window will be assessed during the following work period.] All cameras are to be reviewed for operability and clarity of view, day, and night.

a. The endurance test must demonstrate system reliability and operability. The endurance test will not be started until the Government notifies the Contractor, in writing, that the system acceptance test is satisfactorily completed, and correction of all outstanding deficiencies has been satisfactorily completed.

b. Provide 1 operator to operate the system 24 hours per day in addition to any Government personnel that may be made available. The Government may terminate testing at any time if the system fails to perform as specified.

c. Upon termination of testing by the Government or by the Contractor, commence an assessment period as defined in paragraph Test Termination Assessment Period. Verify the operation of each terminal device during the last day of the test. Upon successful completion of the endurance test, deliver test reports and other documentation as specified to the Government prior to acceptance of the system.

d. The endurance test for sensors is required to demonstrate the configuration meets the requirements of Section 28 10 05 ELECTRONIC SECURITY SYSTEMS (ESS) paragraphs False Alarm Rate and Nuisance Alarm Rate. The Government Representative must be directly notified if any section of the fence exceeds the requirement. Upon coordination, re-calibrate the failed section, repeat functional test, and restart the endurance test period for that section.

3.4 FINAL TEST REPORT

Submit a Final Test Report following the successful completion of acceptance testing to include all failures, remediation, and resolution of all punch list items. Address the following topics in the Final Test

Report:

3.4.1 Summary

Provide a chronological summary of all testing. Describe test activities and results in narrative form.

3.4.2 Personnel

Provide a list of all Contractor and Government personnel who participated in the testing.

3.4.3 Test Logs

Provide all completed test logs along with a test log verification signed by the Test Director.

3.4.4 False and Nuisance Alarm Rates

Provide a tabulated and summarized listing of all events based on the system activity reports. Categorize every alarm as one of four types: 1) Valid/Actual, 2) False, 3) Nuisance, or 4) Test/Authorized Alarm.

3.4.4.1 Valid or Actual Alarm

An alarm received due to an actual intruder attempting to enter or entering a protected area or attempting to cross or crossing a line of detection.

3.4.4.2 False Alarm

An alarm received for which no cause can be determined. Typically, false alarms are due to aging or malfunctioning equipment and communications pathways that the alarm monitor cannot assess. False alarms in excess of established rates will cause complacency and lead to unsecure protected areas.

3.4.4.3 Nuisance Alarm

An alarm received due to an influence for which the sensor was designed to detect but which is not related to an intrusion attempt. The influence that caused the alarm must be clearly identifiable. These alarms fall into three categories: preventable, mitigatable, and unpreventable. Preventable nuisance alarms typically include personnel using improper entry/exit procedures, or an unauthorized incursion into the sensor zone. Preventable nuisance alarms must be included in the nuisance alarm rate. Mitigatable nuisance alarms can include: an animal entering into the sensor zone; a weather event typical/normal to the area, a noise event (i.e., a jet taking off in afterburner, a training explosion from the base range, etc.), or a seismic event (large vehicle vibrations from regular traffic in the area). Steps must be taken to reduce mitigatable events such as critter/animal control fences or animal abatement, bird abatement programs such as Bird/wildlife Aircraft Strike Hazard (BASH) or reprograming the system to filter out certain vibrations/noises. Mitigatable nuisance alarms must be included in the nuisance alarm rate. Unpreventable nuisance alarms can include a weather event not typical/normal to the area (i.e., thunderstorm, hurricane, typhoon, etc.) or other atypical events to the area and will not be included in the nuisance alarm rate. Nuisance alarms in excess of established rates will

cause complacency and lead to unsecure protected areas.

3.4.4.4 Test or Authorized Alarm

An alarm received due to authorized personnel performing required testing on the ESS. Tests can include daily, weekly, or monthly operational checks as well as acceptance, quarterly, semi-annual, or annual system functional checks.

3.5 Probability of Detection and Confidence Level

If Probability of Detection (Pd) requirements need to be validated, then Pd testing must be completed. The binomial table below uses a statistical method to determine Pd and Confidence level based on the number of sequential annunciated alarms due to test intrusions. Regulatory or contractual requirements will define the Pd and Confidence Level needed for specific zones or lines of detection. If the number of successive detections cannot be met without a missed detection, then adjustments to detection sensor coverage and sensitivity must be made.

Probability of Detection	0.9	0.9	0.95	0.95	Number of Misses Allowed
Confidence Level	90%	95%	90%	95%	
Number of Intrusion Attempts	22	29	45	59	0
	38	46	77	93	1
	52	61	105	124	2
	65	76	132	153	3
	78	89	158	181	4
	91	103	184	208	5

-- End of Section --