FROM: HQ AFCESA/CEO
139 Barnes Drive Suite 1
Tyndall AFB FL 32403-5319

SUBJECT: Engineering Technical Letter (ETL) 11-1: Civil Engineer Industrial Control System Information Assurance Compliance

1. Purpose. This ETL provides technical guidance and criteria for information assurance (IA) of civil engineering (CE) industrial control systems (ICS). This ETL applies to all ICSs that utilize any means of connectivity to monitor and control industrial processes, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC), which are often found in industrial equipment and critical infrastructures.

Note: The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this ETL does not imply endorsement by the Air Force.

2. Application. This ETL supersedes ETL 09-11, Civil Engineering Industrial Control System Information Assurance Compliance, dated October 26, 2009. Requirements in this ETL are mandatory. The interpreting authority for this ETL is the Air Force Civil Engineer Support Agency, Operations and Programs Support Division, Engineer Support Branch (HQ AFCESA/CEOA).


2.2. Effective Date: Immediately.

2.3. Intended Users:
- Major command (MAJCOM) engineers
- Base civil engineers (BCE)
- ICS information assurance managers (IAM)

2.4. Coordination:
- MAJCOM engineers responsible for CE ICSs
- The Air Force Civil Engineer, Resources Division, Information Technology Branch (HQ AF/A7CRT)
- Air Force Network Integration Center, Information Assurance Directorate (AFNIC/EV) and Air Force certifying authority (CA)
- Chief, Cyberspace Surety Division (SAF/A6OI), on behalf of Director, Cyberspace Operations (SAF/A6O) and Air Force senior information assurance officer (SIAO)

APPROVED FOR PUBLIC RELEASE: DISTRIBUTION UNLIMITED
3. Referenced Publications.


- Air Force policy directive (AFPD) 16-14, Information Protection
- AFI 31-401, Information Security Program Management
- AFI 31-501, Personnel Security Program Management
- AFI 32-1063, Electric Power Systems
- AFI 33-112, Information Technology Hardware Asset Management
- AFI 33-114, Software Management
- AFI 33-115V1, Network Operations (NETOPS)
- AFI 33-115V2, Licensing Network Users and Certifying Network Professionals
- AFI 33-200, Information Assurance (IA) Management
- AFI 33-210, Air Force Certification and Accreditation (C&A) Program (AFCAP)
- AFI 33-230, Information Assurance Assessment and Assistance Program
- AFNIC EV 2010-08, Guide for Submission of Platform Information Technology (PIT) Determination Concurrence Requests, 18 August 2010
- Information Technology Investment Policy Guidance Memorandum, 9 June 2008, HQ USAF/A7C


3.4. Department of Defense (DOD):

3.5. National Institute of Standards and Technology (NIST):

3.6. Other Government References:


5. Background.

5.1. ICS Overview.

5.1.1. Industrial control system (ICS) is a general term for several types of control systems, including SCADA systems, DCSs, and other control system configurations such as skid-mounted or panel-mounted PLCs often found in the industrial sector and critical infrastructure. ICSs are typically used in infrastructure/utility/industrial systems such as electrical, water and wastewater, oil and natural gas, chemical, transportation, pharmaceutical, pulp and paper,
food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods).

5.1.1.1. SCADA systems are highly distributed systems used to control geographically dispersed assets, often scattered over thousands of square miles, where centralized data acquisition and control are critical to system operation. SCADA systems are used in distribution systems such as water distribution and wastewater collection systems, oil and natural gas pipelines, electrical power grids, and railway transportation systems.

5.1.1.2. DCSs are used to control industrial processes such as electrical power generation, oil refineries, water/wastewater treatment, and manufacturing production. DCSs are integrated as a control architecture containing a supervisory level of control overseeing multiple integrated subsystems responsible for controlling the details of a localized process.

5.1.1.3. PLCs are computer-based, solid-state devices controlling almost all industrial equipment and processes. While PLCs are control system components used throughout DCS and SCADA systems, PLCs are often the primary components in smaller control system configurations used to provide operational control of separate processes.

5.1.2. For Air Force CE, real property ICSs include, but are not limited to, the following types of systems (including all points, devices, control panels, means of connectivity, software, controllers, computer workstations, servers, etc.):

- Supervisory control and data acquisition (SCADA) systems
  - Fuel distribution systems
  - Protective relays
  - Cathodic protection systems
  - Power generation systems, including renewable systems
  - Natural gas distribution systems
- Energy management and control systems (EMCS)
- Automated meter reading (AMR)/utility systems, including water metering systems
- Fire alarm/fire suppression/mass notification systems
- Utility monitoring and control (UMAC) systems
  - Electrical distribution systems
  - Generator monitoring systems
  - Water system controls
  - Natural gas distribution systems
- Airfield control systems
  - Lighting system controls
  - Aircraft arresting system (AAS) controls
- Traffic signal controls and vehicle barriers
• CE-maintained intrusion detection systems (IDS) (by CE/Security Forces memorandum of agreement only). **Note:** IDSs are not considered real property installed equipment.

5.1.3. Initially, many CE ICSs had little resemblance to traditional information technology (IT) systems in that ICSs were isolated systems running proprietary control protocols using specialized hardware and software. Widely available, low cost Internet Protocol (IP) devices are now replacing proprietary solutions, which increases the possibility of cyber security vulnerabilities and incidents. As ICSs are adopting IT solutions to promote corporate business systems connectivity and remote access capabilities, and are being designed and implemented using industry standard computers, operating systems, and network protocols, ICSs are starting to resemble IT systems. This integration supports new IT capabilities, but it provides significantly less isolation for ICSs from the outside world than predecessor systems, creating a greater need to secure these new systems. While security solutions have been designed to deal with these security issues in typical IT systems, special precautions must be taken when introducing these same solutions to ICS environments. In some cases, new security solutions are needed that are tailored to the ICS environment.

5.1.4. Many ICS characteristics differ from those of traditional IT systems, including different risks and priorities. Some of these ICS characteristics include significant risk to the health and safety of human lives and serious damage to the environment. ICSs have different performance and reliability requirements and use operating systems and applications that may be considered unconventional to typical IT support personnel. Furthermore, the goals of safety and efficiency can sometimes conflict with security in the design and operation of control systems. For example, requiring password authentication and authorization should not hamper or interfere with emergency actions for the ICS. For additional information concerning the distinct differences between ICSs and typical IT systems, see NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security*, section 3.1.

5.2. Information Assurance (IA) of ICSs.

5.2.1. The Air Force Chief Information Officer (CIO) has issued policy guidance for the identification and IA of all legacy and future information systems (IS). For the CE community, these systems include the ICSs identified in paragraph 5.1.2 whether or not they are physically connected to the base local area network (LAN) or Air Force Global Information Grid (AF-GIG). ICSs that do not have a direct connection to the AF-GIG (see Attachment 2 for definition) are considered platform IT (PIT) systems. If a connection to the AF-GIG exists, that connection is considered a PIT interconnection (PITI).
5.2.2. Platform IT (PIT) Systems.

5.2.2.1. A PIT system is considered a special purpose system using computing resources (i.e., hardware, firmware, and [optionally] software) that are physically embedded in, dedicated to, or essential in real time to the mission performance of the system. A PIT system performs only (i.e., is dedicated to) the information processing assigned to the PIT system by its hosting special purpose system. Examples include, but are not limited to, SCADA-type systems, certain medical devices, training simulators, and diagnostic test and maintenance equipment.

Note: PIT point-to-point interconnections using an Air Force installation’s backbone infrastructure for the purpose of connecting to remote sensors or to another PIT capability (within the same base/enclave) are not considered to be PITIs as long as they are logically or physically separated/isolated from the base common user infrastructure and systems (see AFNIC EV 2010-08, Guide for Submission of Platform Information Technology (PIT) Determination Concurrence Requests). See section 8.1.6 of this ETL for additional guidance on virtual local area networks (VLAN).

5.2.2.2. ICS PIT Certification and Accreditation (C&A). ICS PIT C&A is required for any new or existing ICS. ICS PIT C&A is not to be confused with the Air Force Certification and Accreditation Program (AFCAP) that utilizes the Defense Information Assurance Certification and Accreditation Process (DIACAP). The ICS PIT C&A process is illustrated in Attachment 1, with step-by-step instructions provided in section 7. New system acquisitions must incorporate security and IA requirements into the design specifications, and systems already in operation require IA controls as prescribed in current policy and guidance. PIT systems require IA risk assessment (RA) and periodic review as directed by the PIT designated accrediting authority (DAA).

5.2.3. Platform IT Interconnections (PITIs).

5.2.3.1. A PITI is the interface/connection between a PIT and the AF-GIG or any other DOD communications network. Examples of PITIs that require security considerations include, but are not limited to, PIT communications interfaces for data exchanges with the AF-GIG for mission planning or execution, remote administration, remote sensing, remote alerting (including one-way communication), and remote upgrade, query, or reconfiguration.

5.2.3.2. PITI C&A.

5.2.3.2.1. When a PIT system requires connection to the AF-GIG or any other DOD network to exchange information as part of the mission of the ICS, the IA requirements for the exchange must be explicitly addressed as part of the interconnection. These interconnections are subject to the
AFCAP and DIACAP as outlined in AFI 33-210, *Air Force Certification and Accreditation (C&A) Program (AFCAP)*, and DODI 8510.01, *DOD Information Assurance Certification and Accreditation Process (DIACAP)*, respectively.

**5.2.3.2.2.** PITI C&A requires documenting any additional measures required by the AF-GIG to extend IA services or to protect the PIT from interconnection risk. The IA controls and level of robustness must be selected as applicable and shall consider the mission assurance category (MAC) and confidentiality level of both the PIT and its interconnecting means. IA controls provide a common management language for establishing IA needs, promoting consistency for testing and validating the implemented IA solutions, reducing complexity when managing changes to the validated baseline, providing a common pivot point when negotiating interconnections, and increasing accuracy for reporting IA readiness.

**Note:** IA controls listed in DODI 8500.2, *Information Assurance (IA) Implementation*, and NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, Appendix I (“Industrial Control Systems”), are designed to complement each other in addressing the uniqueness of PIT or PITI. When IA controls conflict, the MAC of the interconnected system will drive the security objectives of the PIT or PITI ICS.

**Note:** All IT is subject to IA policy, but PIT is excluded from the AFCAP; however, **PITIs** are specifically subject to the AFCAP, per AFI 33-210.

**5.2.4.** Figure 1 shows the applicability of IA policy for PIT systems and IA policy and the AFCAP for PITIs to the AF-GIG.

6.1. Within CE are base-level ICS IAMs, MAJCOM ICS functional area managers (FAM), the ICS program manager (PM), the ICS PIT certifying authority (CA), the ICS portfolio manager (PfM), and the ICS PIT DAA. Their general roles, responsibilities, and qualifications are as follows:

6.1.1. Base-level ICS IAM. The BCE shall appoint, in writing, a primary and alternate ICS IAM for the civil engineer group (CEG) or civil engineer squadron (CES). The ICS IAMs are responsible for ensuring that base CE ICSs are certified and accredited in accordance with DOD and Air Force IA directives and instructions.

6.1.1.1. The primary ICS IAM must have Information Assurance Technical (IAT) Level II or Information Assurance Management (IAM) Level I certification in accordance with DOD 8570.01-M, Information Assurance Workforce Improvement Program, within six months of BCE appointment. (Note: Security+ certification satisfies either IAT Level II or IAM Level I certification.) If the CEG or CES has IT support personnel, it is recommended that the BCE assign an IT system administrator as the primary ICS IAM. Many Air Force CE IT specialists have IAT Level I or higher certification. In addition to the primary ICS IAM, an alternate ICS IAM must be appointed to assist the primary with the functional and technical aspects of ICSs. The alternate ICS IAM must be a qualified ICS operator/technician, and IAT/IAM certification is desired but not required. The alternate ICS IAM’s primary role is to provide the necessary technical support/expertise to the primary ICS IAM to achieve ICS IA certification and accreditation. These two individuals will leverage each other’s expertise to achieve IA of our ICSs.

6.1.1.2. The primary ICS IAM shall:
- Approve and manage all access privileges to ICS software and systems; validate all access privileges annually; and re-evaluate frequency requirements every three years or at any mission change, system change, or other significant change to operating requirements.
- Ensure appropriate access privileges for all individuals based on their training, qualification, and functional duties.
- Manage CE ICS access by ensuring that accounts are deactivated or activated in a controlled manner. Personnel designated to make configuration decisions and responsible for IA controls for both PIT and PITI shall be certified to IAT Level II or IAM Level I in accordance with DOD 8570.01-M.
- Have full administrative rights to install software updates/patches.
- Have access to review, modify, and edit the Enterprise Information Technology Data Repository (EITDR) entries as approved by the ICS FAM.
• Document and track system configurations for each CE-owned, -operated, and -maintained ICS throughout the system life cycle, including any Air Force CE ICSs operated and maintained by contractors. For each ICS, the ICS IAMs will assemble a PIT determination package in accordance with section 7.1.1 of this ETL and forward the package to the respective ICS FAM.

• Provide an annual report entitled “Industrial Control System Security Status Report” to the MAJCOM ICS FAM. The report will include a summary of current systems and system changes and will indicate compliance/non-compliance with IA security requirements. This report is due to the ICS FAM in October of each year.

6.1.1.3. The alternate ICS IAM shall:

• Document and track system configurations for each CE-owned, -operated, and -maintained ICS throughout the system life cycle, including any Air Force CE ICSs operated and maintained by contractors. For each ICS, the ICS IAMs will assemble a PIT determination package in accordance with section 7.1.1 of this ETL and forward the package to the respective ICS FAM.

• Provide an annual report entitled “Industrial Control System Security Status Report” to the MAJCOM ICS FAM. The report will include a summary of current systems and system changes and will indicate compliance/non-compliance with IA security requirements. This report is due to the ICS FAM in October of each year.

6.1.2. MAJCOM ICS FAM. The ICS FAM is designated in writing by the MAJCOM A7O (Operations) or equivalent. The ICS FAM is responsible for collecting the base-level PIT determination packages, reviewing them for completeness, and sending them to the ICS PM. In addition, the ICS FAM will submit an annual report entitled “Industrial Control System Security Status Report” to the ICS PfM. This report will contain a summary of current systems and system changes and will indicate compliance/non-compliance with IA security requirements. This report is due in November of each year. The ICS FAM may have access to create, modify, or delete EITDR entries as approved by the ICS PM or ICS PfM.

6.1.3. ICS PM. The ICS PM is designated in writing by HQ AFCESA/CEO. The ICS PM is responsible for ensuring appropriate scheduling of all IA aspects of the program to meet the ultimate goals of IA compliance. The ICS PM is also responsible to ensure that the following tasks are accomplished:

• Review and submit ICS PIT packages to Air Force CA for a PIT determination statement.
• Complete initial EITDR entries for CE ICS PITs.
• Provide updates to MAJCOM FAMs on the status of C&A activities of their respective systems.
• Establish a PIT integrated product team (IPT) of engineers, testers, etc.
• Coordinate and oversee execution of IA RAs.
• Ensure that all IA testing requirements are performed.

6.1.4. ICS PIT CA. The PIT CA is the technical authority for the IA aspects of a PIT system within their control. The PIT CA is responsible for ensuring clear definition of the IA requirements at the earliest stage possible. The PIT CA is then responsible for ensuring the implementation of the IA requirements to the extent possible based on program or system cost, schedule, and technical trade-offs. One of the primary functions of the PIT CA is to review the RA completed by the IPT. The ultimate goal of the RA is to mitigate or reduce remaining risks to an acceptable level. The PIT CA should agree with the RAs and help structure any mitigations for those risks not considered low. The PIT CA has the responsibility to advise the PIT DAA in making a final IA RA of the system. The PIT CA is designated in writing by the Air Force SIAO. The Air Force SIAO has designated HQ AFCESA/CEO as the ICS PIT CA.

6.1.4.1. The ICS PIT CA may have the following roles and responsibilities:
• Act as the focal point for the CE ICS IA compliance program and ETL.
• Coordinate CE ICS IA-related tasks with ICS PfM/ICS PIT DAA.
• Review and approve CE ICS IA strategy and implementation.
• Act as the technical authority for ICS-related IA issues.
• Certify the ICS IA design and implementation.
• Advise the ICS PIT DAA on IA-related issues.

6.1.4.2. Technical aspects of an ICS that may be reviewed include the following:
• ICS IA requirements
• Threat assessments
• Accreditation boundary/demilitarized zone (DMZ)
• Topology, block, and data flow diagrams
• Software, hardware, and firmware analysis
• Network connection compliance analysis
• Integrity analysis of integrated products
• Risk/vulnerability assessment results/findings
• Mitigation recommendations/techniques/shortfalls

6.1.4.3. Air Force SIAO-Directed Training, Certification, and Reporting Requirements:
• Maintain compliance with training and certification criteria outlined in National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4015, National Training Standard for System Certifiers, and DOD 8570.01-M.
• Submit monthly reports to SAF/A6OI providing the status of all HQ AF/A7 CE ICS certified over the specified period at af.infoassurance@pentagon.af.mil.

6.1.5. ICS PfM. The ICS PfM has oversight responsibility for IT initiatives and systems for which they have lead funding responsibility. The ICS PfM is required to certify to the Air Force CIO annually, based on the ICS security status reports received from the ICS FAMs, that the provided IT portfolio management information is complete, accurate, and in accordance with current Air Force IT portfolio management direction as provided in budgetary documents (policy, annual planning and programming guidance, program objective memorandum preparation instructions, etc.). The ICS PM assists the ICS PfM by ensuring that all ICSs are registered in the EITDR. The ICS PfM resides at HQ AF/A7CRT and is responsible for CE portfolio management and annual reviews to maximize the value of IT investments and minimize the risk.

6.1.6. ICS PIT DAA. The PIT DAA is designated in writing by the Air Force CIO. The PIT DAA has a level of authority commensurate with accepting, in writing, the risk of operating all PIT systems under their jurisdiction. The PIT DAA must be independent of any particular program, but has the authority to influence programs from a global perspective. The PIT DAA consults with the PIT CA in making decisions but is not bound by the recommendation of the PIT CA. The PIT DAA takes into account the command’s technical and programmatic needs in rendering a decision. The Air Force CIO has designated HQ AF/A7C-2 as the CE ICS PIT DAA. See Attachment 3.

6.1.6.1. ICS PIT DAA Responsibilities. The PIT DAA may have the following responsibilities:

• Ensure that IA requirements are identified and integrated into the systems engineering and acquisition processes as appropriate.
• Review/approve the accreditation decision package that includes an IA RA and mitigation approach.
• Accredit/deny systems for test or operation.
• Submit the system accreditation package to the Air Force DAA for network connection to the AF-GIG (if required) and acknowledge any PITIs in their accreditation decisions.

6.1.6.2. ICS PIT DAA Decisions. The PIT DAA may grant the following accreditation decisions to PIT ICSs under their purview:

1. Interim Authority to Test (IATT): Special case for authorizing testing in an operational environment or with live data for a specified time period. An IATT is for testing purposes only.
2. Interim Authority to Operate (IATO): A temporary authorization to operate under the conditions or constraints enumerated in the accreditation decision. An IATO is normally granted for up to
180 days. The DAA may not grant consecutive IATOs totaling more than 360 days.

3. Authority to Operate (ATO): Accreditation by the DAA for the system to operate without restriction. All IA risks are considered low or mitigations are in place, and the DAA agrees that any residual risk is acceptable under the circumstances. An ATO is required prior to initial operating capability (IOC). An ATO may be granted up to three years.

4. Denial of Authorization to Operate: A DAA decision that the information system cannot operate because of inadequate IA design, failure to adequately implement assigned IA requirements, or lack of adequate security.

6.1.6.3. Air Force CIO-Directed Training, Certification, and Reporting Requirements:

- Complete training and maintain appropriate IA certification in accordance with DOD 8570.01-M, Chapter 5, and Committee on National Security Systems Instruction (CNSSI) No. 4012, *National Information Assurance Training Standard for Senior System Managers*, prior to appointment. Proof of training (e.g., certificate) will be included as an artifact to the PIT accreditation decision package.
- Submit semi-annual reports to SAF/A6OI providing the status of all CE PIT ICSs accredited over the specified period at af.infoassurance@pentagon.af.mil.

7. CE ICS C&A Process. The C&A process for PIT systems, with or without interconnections, commences at issuance of this ETL. The C&A process is divided into three phases: Phase 1, ICS PIT Determination; Phase 2, ICS PIT C&A; and Phase 3, PITI AFCAP. Figure 2 summarizes the CE ICS C&A process flow chart provided in Attachment 1.
7.1. Phase 1: PIT Determination.

7.1.1. ICS IAMs shall document system configurations for each CE-owned, -operated and -maintained ICS, including any ICS operated and maintained by contractors. For each ICS, the ICS IAM will assemble a PIT determination package composed of the following information and forward that package to the respective ICS FAM.

7.1.1.1. Provide a single line block diagram of each type of ICS architecture. These diagrams should show the ICS network topology (i.e., its interconnections, data flow, components, and external connections).

- System connectivity
  - How the data flows
  - Where the data is coming in and out
  - Connection type(s) – wireless radio frequency (RF), Cat5, fiber, modem, etc.
  - Firewall location(s), if applicable
- System interconnectivity (i.e., other systems to which the ICS is connected, whether PIT, PITA, commercial Internet service provider, World Wide Web (WWW), GIG, LAN, etc.)
- Key components, including:
  - Make and model
  - IP address, if applicable
- Accreditation boundary (or boundaries), DMZ, or security boundary. The ICS security boundary shall be identified and well defined on all single line diagrams and network topologies for each ICS. The ICS
security boundary is the demarcation of connection to the AF-GIG or other DOD network.

- Firewalls, if applicable
  - Vendor, make, model, software version
- Cyber intrusion prevention/detection, if applicable
  - Vendor, make, model, software version
- IP addresses, if applicable. Do not use Xs. Network and ranges must be expressed correctly.

**Note:** The diagram must allow the Air Force CA to clearly understand and identify the hardware, software, and other IT components as well as the mission the platform supports.

7.1.1.2. Complete the Modified DIACAP Implementation Plan (MDIP) template for each ICS (see paragraph 5.1.2 for a list of common ICSs). Include any ICS architecture and installation specifications for each type of ICS architecture.

**Note:** ICS architecture and installation instructions are typically provided by the vendor and can be supported through vendor-specific literature, white papers, and/or configuration guides.

7.1.1.3. Complete the PIT determination checklist. This data is required by the ICS PM for input into the EITDR.

7.1.1.4. Describe the ICS in narrative form, and describe how, in real time, the ICS supports the operation and functionality of the special purpose system.

7.1.1.5. Submit the above information to the ICS FAM via a digitally signed and encrypted e-mail message.

7.1.2. ICS FAMs should submit the packages to the ICS PM via an encrypted and digitally signed e-mail message.

7.1.3. The ICS PM reviews the PIT(I) determination packages for completeness and submits them to the Air Force CA for a PIT(I) determination. The ICS PM will request in writing an Air Force CA evaluation to determine if the ICS is PIT(I). If the ICS requires the use of interconnections not connected to the AF-GIG, the ICS PM must state the justification for requesting exemption from the AFCAP, including rationale for the ICS as PIT.

7.1.4. The Air Force CA will evaluate the package and determine if the ICS is PIT. If the Air Force CA determines that the submission represents PIT, the PIT determination letter will indicate concurrence that the ICS meets the criteria for designation as PIT and is exempt from the formal AFCAP. Non-concurrence by the Air Force CA means the system is not a PIT system or the system has an
interconnection to the AF-GIG. The AFCAP will be required for those systems and interconnections in accordance with AFI 33-210.

7.1.5. The ICS PM shall receive the PIT(I) determination letter from the Air Force CA, review for changes to the original ICS architecture, recommend best security practices using, as a minimum, NIST SP 800-53, Appendix I, and provide additional instructions for Phase 2 of the CE ICS C&A process. The ICS PM will also provide system security and IA strategies.

7.1.5.1. If the ICS PM does not agree with the Air Force CA’s PIT determination, the ICS PIT CA may appeal Air Force CA’s determination to the Air Force SIAO for reconsideration. The Air Force SIAO’s decision is final. If the ICS PM does not wish to appeal Air Force CA’s determination, then the ICS PM will update the PIT package indicating PITI reclassification to the ICS PfM and to the ICS FAM.

7.1.5.2. The ICS PM will forward to the ICS FAM the Air Force CA PIT(I) determination statement, proposed security requirements, and IA controls required for each approved PIT(I) ICS. The ICS PM will enter the system into the EITDR with assistance from the ICS PfM.

7.1.6. Upon receipt of the PIT(I) determination statement, the ICS FAM will notify the respective ICS IAMs of the Air Force CA’s determination and any required security actions. Transition to Phase 2 of the CE ICS C&A process is now authorized.

7.2. Phase 2: ICS PIT C&A.

7.2.1. The ICS PM will provide the ICS PIT CA with an overview of, and any changes to, the CE ICS C&A process. PIT CA approval of the RA strategy, templates, tools, and test team activation is required prior to scheduling and supporting site visits at active and reserve bases. The Civil Engineer Maintenance, Inspection, and Repair Team (CEMIRT) currently provides, among other areas of expertise, ICS technical support to the ICS PIT IPT. That support is expanding to include CEMIRT RA teams to help base ICS IAMs assess ICS threats, vulnerabilities, and risks. CEMIRT will also identify, implement, and/or recommend risk mitigation strategies, techniques, and/or solutions. The CEMIRT RA team will generate an IA RA and mitigation report within two weeks after the RA. CEMIRT will not coordinate and schedule site visits until all site-specific PIT determination statements are received from the Air Force CA, thus preventing multiple site visits.

7.2.2. The ICS PM goal will be to review and validate the IA RA and mitigation report and assemble the accreditation decision package (ADP) for the PIT CA within 30 calendar days of receipt.
7.2.3. The PIT CA will review the ADP and submit a recommendation to the PIT DAA for consideration.

7.2.4. The PIT DAA will issue an ATO once all compliance actions are certified by the PIT CA. An IATO may be issued at the PIT DAA’s discretion prior to a formal ATO to reduce or eliminate known risks/vulnerabilities. If the PIT DAA issues an IATO or ATO, the ICS FAM and ICS IAM will be provided with a copy of the C&A approval, and the ICS IAM is responsible for continuously monitoring the approved PIT configuration as defined in the PIT package for security compliance of the ICS and for making EITDR updates as necessary or as prescribed by the ICS FAM. Changes in submitted topology or component configuration shall be staffed to the ICS PM for approval prior to implementation.

7.3. Phase 3: ICS PITI C&A.

7.3.1. If the PIT system has a previously identified interconnection to the AF-GIG, the formal AFCAP commences. The AFCAP will not begin until the PIT receives an IATO or ATO. The ICS PM will submit the entire package, with the proposed system design or legacy system interface description, along with the ICS PIT DAA signed ATO letter, to the Air Force CA.

7.3.2. Using the ICS system configuration submittals from the ICS FAM, the ICS PM and ICS PfM have the responsibility to work together and submit the package for C&A in accordance with AFI 33-210. If the ICS requires an on-site evaluation to validate IA controls, an IATT will be requested and submitted as part of the C&A package.

7.3.3. If the Air Force DAA/CA issues ATO and authority to connect (ATC) for the PITI, the ICS PM shall work with the ICS FAM and ICS IAM to implement any additional security actions to meet established AFCAP requirements (i.e., continuous monitoring and annual FISMA reporting requirements). The ICS IAM is responsible for maintaining accreditation and security for each ICS PITI. If the Air Force DAA and/or the Air Force CA disapproves interconnect, instructions/directions/rationale will be provided to the ICS PIT DAA and ICS PIT CA for corrective action.

8. Technical Requirements. This section outlines hardware and operational requirements for existing and new PIT ICSs and for existing PITI ICSs to operate while awaiting C&A and/or AFCAP approval.

8.1. Base-level ICS IAMs shall ensure that ICSs comply with the requirements in the following paragraphs. The MAJCOM ICS FAM is responsible for technical oversight of the requirements in this section of the ETL and shall consult with the HQ AFCESA ICS PM for clarification or interpretation of these requirements.
Note: ICSs on OCONUS military installations (outside the continental United States and its possessions [US&P]) or military installations not owned or operated by the DOD are installed and maintained under the rules and regulations of the host nation government. Personnel granted access to these systems shall comply with host nation and Air Force minimum training and experience requirements. Waivers to this policy require approval from the BCE, installation commander, MAJCOM CE, HQ AFCESA/CC, and the host nation governing body.

Note: For certification of supporting ICSs under host nation control and/or ownership, identify the ICS and forward technical information through the ICS FAM to the ICS PM for further guidance.

8.1.1. Because of inherent security risks, all commercial wireless networking devices are considered “external” connections to both PIT and PITI systems and warrant additional scrutiny before being implemented into the ICS architecture.

8.1.1.1. At a minimum, any data transmitted by commercial wireless devices, services, and technologies will implement data encryption from end to end over an assured channel (AC) (see clarification in Note below) and shall be validated under the Cryptographic Module Validation Program as meeting requirements, per Federal Information Processing Standards Publication (FIPS PUB) 140-2, Security Requirements for Cryptographic Modules, Overall Level 1 or Level 2, as dictated by the sensitivity of the data. Historically, ICS devices were not designed with encryption capabilities. In cases where commercial wireless must be employed but the ICS device(s) cannot provide FIPS PUB 140-2 encryption capabilities, the architecture must be carefully designed to provide an AC and additional defense-in-depth risk mitigation strategies to complement the IA controls to achieve an adequate level of security. The minimum acceptable cryptographic standard is the Advanced Encryption Standard (AES) using a cryptographic key length of 128 bits as outlined in FIPS PUB 197, Advanced Encryption Standard (AES).

Note: To clarify, an AC is a network communication link protected by a security protocol providing authentication, confidentiality, and data integrity, and employs US government-approved cryptographic technologies whenever cryptographic means are used. Examples of protocols and mechanisms sufficient to meet the requirements of authentication, confidentiality, and data integrity protection for an AC are Internet Protocol Security (IPSec); Secure Sockets Layer (SSL) v3; Transport Layer Security (TLS); and systems using National Security Agency (NSA) -approved high assurance guards with link encryption methodology.

Exception: Fire alarm reporting systems do not require data encryption for signaling to/from the fire alarm control panel (FACP). See paragraph 8.1.5.3 for requirements for sensitive compartmented information facilities (SCIF).
8.1.1.2. Substituting wireless for wired technology introduces numerous vulnerabilities into the network, which may be unacceptable or not cost-effective to mitigate. Convenience and/or minimal cost savings shall not be the sole justification for the use of wireless technologies.

8.1.1.3. Adding commercial wireless technologies to an existing approved network configuration boundary is considered a major configuration change and requires a review of security controls and the accreditation decision.

Note: Data hashing, regardless of the method, is not a form of encryption.

8.1.2. Telephone Modems.

8.1.2.1. PIT systems with modem connections to the Defense Switched Network (DSN) require PITI C&A (i.e., AFCAP) on those connections.

8.1.2.2. All telephone modems shall be a secure, dial-back (call-back) type. These exceptions apply:
- Dial-out modems for voice annunciation only are not required to be of the dial-back type.
- Conventional modems over DSN lines are permitted for control of AASs.

8.1.2.3. All telephone modems shall be configured to communicate with on-base or DSN numbers only.

8.1.2.4. Submit a request to the Network Operations and Security Center (NOSC) administrator to block all incoming commercial callers to specific modem control numbers that access ICSs and to block modem dial-out numbers from going off base.

8.1.2.5. The base-level ICS IAM shall provide these numbers to the voice protection system (VPS) personnel at the NOSC.

Note: If the PIT is connecting to one or more phone lines, the phone lines must be identified to the respective NOSC (East, West, Air National Guard). The voice protection team at the NOSC will assist in locking down the point of telephone service (POTS) line to further secure the PIT.

8.1.2.6. Establish audit procedures to record and archive modem usage, blocked calls, and rule violations. This audit record is an IA control and shall be accomplished annually or more often if situations dictate. These records shall be available for a minimum of six years.
8.1.3. ICS passwords shall be as follows:

8.1.3.1. Top-level access portions of the ICS, such as system host or client stations or computers, must comply with the following IA password safeguards.

8.1.3.1.1. Passwords shall not be factory default settings.

8.1.3.1.2. Passwords shall be at least 15 characters in length (for new system acquisitions) or the maximum supportable, using the following criteria:

- Do not use a password that has been used in the past.
- Use a minimum of two numbers, two special characters (e.g., $, %), two capital letters, and two lower-case letters. If special characters are not supported by the ICS, use the broadest combination of password features supported.
- Do not create a password that includes a phone number, home address, birth date, or personal specific dates.
- Do not use a word listed in a dictionary.
- Do not use simple or default passwords (e.g., 1234, data).

8.1.3.1.3. Passwords on all systems shall be changed every 90 days.

8.1.3.1.4. Password control shall incorporate a lock-out requirement.

8.1.3.2. Password-capable field devices (i.e., remote terminal units or field control devices) shall have their passwords changed from manufacturer defaults, and thereafter, as directed by the ICS IAM. The ICS IAM shall provide written certification to the MAJCOM ICS FAM that all password-capable field device passwords have been changed from manufacturer defaults. This certification shall be included as an artifact for final accreditation as PIT or PITI.

8.1.4. Radios used on any wireless ICS within the US&P that will transmit/receive within the Federal or military spectrum require frequency approval from base-level spectrum managers. A DD Form 1494, Application for Equipment Frequency Allocation, commonly referred to as the J-12 process, shall be approved before a spectrum allocation is issued. If the ICS uses an unlicensed frequency that complies with Federal Communications Commission (FCC) Part 15B (see Title 47 CFR, Part 15, Radio Frequency Devices), notify the base-level spectrum manager of the use of this unlicensed frequency. If a wireless solution is proposed for use outside the US&P, the MAJCOM ICS FAM shall contact the MAJCOM spectrum manager for host nation approval.

8.1.4.1. Develop contingency plans to manually control ICSs when RF interference disrupts monitoring or control.
**Note:** Non-licensed device operations must accept any interference from any Federal or non-Federal authorized radio station, other non-licensed devices, or industrial, scientific, and medical (ISM) equipment. The agency operating a non-licensed device that causes interference to an authorized radio station shall promptly take steps to eliminate the interference. Upon notification by the base spectrum manager that the device is causing interference, the operator of the non-licensed device shall cease all radiations from the device. Operations shall not resume until the condition causing the interference has been corrected.

**Note:** Non-licensed devices, since they operate on a non-interference basis, may not provide sufficient reliability for critical radio communications functions affecting human life or property; however, non-licensed devices may provide valuable and unique supplemental or expendable radio communications services where needed. To ensure adequate regulatory protection, Federal entities should rely only on devices with frequency assignments in the Federal or military spectrum and in the government master file as principal radio communication systems for safeguarding human life or property.

8.1.4.2. Any wireless transmission in the 2.4 gigahertz (GHz) unlicensed frequency range that is not a Combat Information Transport System Program Management Office (CITS PMO) -installed access point should be coordinated with the CITS lead command, AFNIC (afnic.ecnn@us.af.mil, (618) 229-5666), for possible interference.

8.1.5. Fire Alarm Reporting Systems.

8.1.5.1. Manually connect/disconnect remote system access (RSA) on all FACPs and/or servers (e.g., D-21) when RSA actions are needed/complete. Section 8.1.2 of this ETL identifies modem connection requirements.

8.1.5.2. Communications modems shall comply with section 8.1.2.

8.1.5.3. Fire alarm reporting from any SCIF to FACPs shall be wired (e.g., copper, fiber) systems, not wireless, and require an (air gap) isolation device if the available notification appliance device is a speaker. Fire alarm reporting signals sent from the SCIF FACP to the central monitoring station must be encrypted.

8.1.6. Virtual Local Area Networks (VLANs).

8.1.6.1. VLANs divide physical networks into smaller logical networks to increase performance, improve manageability, and simplify network design. VLANs are achieved through the use of managed Ethernet switches. A managed switch provides all the features of an unmanaged switch, plus the ability to configure the switch to allow greater control over how the data
travels over the network and who has access to it. Each VLAN consists of a single broadcast domain that isolates traffic from other VLANs. Just as replacing hubs with switches reduces collisions, using VLANs limits the broadcast traffic, as well as allowing logical subnets to span multiple physical locations. There are two categories of VLANs:

- Static, often referred to as port-based, in which switch ports are assigned to a VLAN so that it is transparent to the end user.
- Dynamic, in which an end device negotiates VLAN characteristics with the switch or determines the VLAN based on the IP or hardware addresses.

8.1.6.2. Although more than one IP subnet may coexist on the same VLAN, the general recommendation is to use a one-to-one relationship between subnets and VLANs. This practice requires the use of a router or multi-layer switch to join multiple VLANs. Many routers and firewalls support tagged frames so that a single physical interface can be used to route between multiple logical networks.

8.1.6.3. VLANs are not typically deployed to address host or network vulnerabilities in the way that firewalls or IDSs are deployed; however, when properly configured, VLANs do allow switches to enforce security policies and segregate traffic at the Ethernet layer. Properly segmented networks can also mitigate the risks of broadcast storms that may result from port scanning or worm activity.

8.1.6.4. Switches have been susceptible to attacks such as media access control (MAC) address spoofing, table overflows, and attacks against the spanning tree protocols, depending on the device and its configuration. VLAN hopping, the ability for an attack to inject frames to unauthorized ports, has been demonstrated using switch spoofing and double tagging. These attacks cannot be conducted remotely and require local physical access to the switch. A variety of features such as MAC address filtering, port-based authentication using IEEE 802.1x, and specific vendor-recommended practices can be used to mitigate these attacks, depending on the device and implementation.

8.1.6.5. VLANs have been deployed effectively in ICS networks, with each automation cell assigned to a single VLAN to limit unnecessary traffic flooding and allow network devices on the same VLAN to span multiple switches. ICSs connected to a VLAN shall incorporate the following:

8.1.6.5.1. Firewalls separating base network traffic from external base traffic and the ICS VLAN. The configuration of the ICS VLAN must ensure that no ICS traffic exits the base firewall.

8.1.6.5.2. Hypertext Transfer Protocol Secure (HTTPS) for remote control of the ICS from the LAN. If Web services are provided to Nonsecure
Internet Protocol Router Network (NIPRNet) systems, implementation of an AC is required.

8.1.7. Replace any unmanaged switch with a managed switch. While awaiting replacement, add physical security measures, house unmanaged switches in a locked secure area, and/or add tamper-proof features. The ICS PM shall approve interim measures.


9.1. Privatized ICSs.

9.1.1. For the purposes of this ETL, privatization is defined as the transfer of ownership and operations of Air Force utility systems and associated industrial monitoring/control systems to the private sector. The private sector includes all privately owned and publicly owned entities.

9.1.2. DOD and Air Force directives and instructions pertaining to IA and DIACAP requirements apply only to DOD-owned systems, including outsourced services such as operation and maintenance (O&M) by a private entity (e.g., Office of Management and Budget (OMB) Circular A-76, Performance of Commercial Activities, outsourced CE O&M or AF Form 9, Request for Purchase, service contract). A privatized utility is no longer a DOD-owned asset, including the privatized ICS that monitors and controls the privatized utility distribution system. Therefore, this formal real estate transaction relieves the US government from any and all planning, financing, designing, constructing, operating, and maintaining responsibilities of this utility infrastructure and associated monitoring and control system.

9.1.3. RF spectrum utilization by a privately owned or publicly owned entity while in garrison requires base or regional spectrum management notification and/or approval.

9.2. Outsourced O&M of ICSs. The following information applies to any OMB Circular A-76 outsourced CE O&M of ICSs, including AF Form 9 service contracts. DOD IA requirements apply to government-owned PIT and PITI ICSs that are operated and maintained by a private entity. Specific guidance for outsourced IT processes is located below and in section 6.9 of DODI 8510.01.

9.2.1. Outsourced IT-based processes that may also support non-DOD users or processes must still be certified and accredited by DOD entities. IA requirements for DOD information in an outsourced environment are determined by the information’s MAC and classification or sensitivity and need to know, just as for other DOD ISs. However, the following also apply:

9.2.2. Technical security of the outsourced environment is the responsibility of the service provider.
9.2.3. Outsourced applications that are accessed by DOD users from DOD enclaves are subject to DOD enclave boundary defense IA controls for incoming traffic (e.g., ports and protocols and mobile code).

9.2.4. Responsibility for procedural and administrative security is shared between the service provider and the supported DOD entity contracting for the service.

9.2.5. The security responsibilities of the service provider down to the control level are made explicit in the contract, along with any other performance and service level parameters by which the DOD shall measure the IA profile of the outsourced IT-based process for the purpose of C&A.

9.2.6. Any baseline IA controls not explicit in the contract or otherwise covered by a service level agreement are categorized as NC. All such NC IA controls must be documented in an IT security plan of action and milestones (POA&M) that explains the acceptability of the risk of operating the outsourced IT-based process with the control in an NC status.

9.2.7. The security roles and responsibilities are to be made explicit in the acquisition, along with the performance and service level parameters by which the DOD shall measure the IA profile of the outsourced IT-based process. The PM for an outsourced IT-based process should carefully define and assess the functions to be performed and identify the technical and procedural security requirements that must be satisfied in the acquisition to protect DOD information in the service provider's operating environment and interconnected DOD ISs.

9.3. Type Accreditation. DODI 8510.01 defines type accreditation as “the official authorization to employ identical copies of a system in specified environments.” This form of C&A allows a single DIACAP package to be developed for an archetype (common) version of an IS that is deployed to multiple locations, along with a set of installation and configuration requirements or operational security needs, that will be assumed by the hosting location. Automated information system (AIS) applications accreditations are type accreditations. Stand-alone IS and DMZ accreditations may also be type accreditations.

9.3.1. HQ AFCESA believes the majority of Air Force ICSs vary greatly in system hardware and software configurations, and consequently, a type accreditation is not warranted.

9.3.2. See AFI 33-210, section 3.14, for additional requirements regarding type accreditations.

9.4. Air Force Civil Engineer IT Investment Policy. In accordance with HQ USAF/A7C’s Information Technology Investment Policy Guidance Memorandum, dated 9 June 2008, all IT investments with functionality supporting a
CE capability must be approved by the A7C IT governance structure prior to any development or sustainment activities or funds being committed or obligated. HQ AF/A7CRT, as the CE CIO, is the office of primary responsibility (OPR) for all CE IT investment processes, including IT portfolio management. The main purpose for the A7C IT governance structure is to analyze, control, select, and evaluate IT investments across the enterprise by standardizing capabilities, reducing duplication, and maximizing functionality across existing IT resources.

10. Points of Contact. The HQ AFCESA ICS PM has interpretive authority for the ICS IA and security issues contained in this ETL. The authority having jurisdiction over the content of this ETL is HQ AFCESA/CEO.

10.1. HQ AFCESA ICS PM. To reach the ICS PM, e-mail AFCESAResearchBackCenter@tyndall.af.mil, call DSN 523-6995 or commercial (850) 283-6995, or mail to 139 Barnes Drive, Suite 1, Tyndall AFB, FL 32403-5319. Subject line: ATTN HQ AFCESA ICS PM.

10.2. HQ AFCESA/CEO. To reach HQ AFCESA/CEO, e-mail AFCESAResearchBackCenter@tyndall.af.mil or afcesa@aetc.af.smil.mil, call DSN 523-6995 or commercial (850) 283-6995, or mail to 139 Barnes Drive, Suite 1, Tyndall AFB, FL 32403-5319.

DAVID J. ANASON, Lt Col, USAF  
Chief, Operations and Programs Support Division  

4 Atchs  
1. CE ICS C&A Process  
2. Acronyms and Terms  
3. CE ICS PIT DAA Appointment  
4. Distribution List
<table>
<thead>
<tr>
<th>Acronyms</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAS</td>
<td>aircraft arresting system</td>
</tr>
<tr>
<td>AC</td>
<td>assured channel</td>
</tr>
<tr>
<td>ADP</td>
<td>accreditation decision package</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>AF-CA</td>
<td>Air Force certifying authority</td>
</tr>
<tr>
<td>AFCAP</td>
<td>Air Force Certification and Accreditation Program</td>
</tr>
<tr>
<td>AF-DAA</td>
<td>Air Force designated accrediting authority</td>
</tr>
<tr>
<td>AF-GIG</td>
<td>Air Force Global Information Grid</td>
</tr>
<tr>
<td>AFI</td>
<td>Air Force instruction</td>
</tr>
<tr>
<td>AFNIC</td>
<td>Air Force Network Integration Center</td>
</tr>
<tr>
<td>AFNIC/EV</td>
<td>Air Force Network Integration Center, Information Assurance Directorate</td>
</tr>
<tr>
<td>AFPD</td>
<td>Air Force policy directive</td>
</tr>
<tr>
<td>AIS</td>
<td>automated information system</td>
</tr>
<tr>
<td>AMR</td>
<td>automated meter reading</td>
</tr>
<tr>
<td>ATC</td>
<td>authority to connect</td>
</tr>
<tr>
<td>ATO</td>
<td>authority to operate</td>
</tr>
<tr>
<td>BCE</td>
<td>base civil engineer</td>
</tr>
<tr>
<td>CA</td>
<td>certifying authority</td>
</tr>
<tr>
<td>C&amp;A</td>
<td>certification and accreditation</td>
</tr>
<tr>
<td>CA</td>
<td>certifying authority</td>
</tr>
<tr>
<td>CCA</td>
<td>Clinger-Cohen Act</td>
</tr>
<tr>
<td>CE</td>
<td>civil engineering</td>
</tr>
<tr>
<td>CEG</td>
<td>civil engineer group</td>
</tr>
<tr>
<td>CEMIRT</td>
<td>Civil Engineer Maintenance, Inspection, and Repair Team</td>
</tr>
<tr>
<td>CES</td>
<td>civil engineer squadron</td>
</tr>
<tr>
<td>CFR</td>
<td>Code of Federal Regulations</td>
</tr>
<tr>
<td>CIO</td>
<td>chief information officer</td>
</tr>
<tr>
<td>CITS PMO</td>
<td>Combat Information Transport System Program Management Office</td>
</tr>
<tr>
<td>Config</td>
<td>configuration</td>
</tr>
<tr>
<td>DAA</td>
<td>designated accrediting authority</td>
</tr>
<tr>
<td>DCS</td>
<td>distributed control system</td>
</tr>
<tr>
<td>DIAACAP</td>
<td>DOD Information Assurance Certification and Accreditation Process</td>
</tr>
<tr>
<td>DMZ</td>
<td>demilitarized zone</td>
</tr>
<tr>
<td>DOD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>DODD</td>
<td>Department of Defense Directive</td>
</tr>
<tr>
<td>DODI</td>
<td>Department of Defense Instruction</td>
</tr>
<tr>
<td>DSN</td>
<td>Defense Switched Network</td>
</tr>
<tr>
<td>EITDR</td>
<td>Enterprise Information Technology Data Repository</td>
</tr>
<tr>
<td>EMCS</td>
<td>energy management and control system</td>
</tr>
</tbody>
</table>
ETL - Engineering Technical Letter
FACP - fire alarm control panel
FAM - functional area manager
FCC - Federal Communications Commission
FIPS PUB - Federal Information Processing Standard Publication
FISMA - Federal Information Security Management Act
GHz - gigahertz
GIG - Global Information Grid
HQ AF/A7C-2 - The Air Force Deputy Civil Engineer
HQ AF/A7CRT - The Air Force Civil Engineer, Resources Division, Information Technology Branch
HQ AFCESA - Air Force Civil Engineer Support Agency
HQ AFCESA/CC - Air Force Civil Engineer Support Agency Commander
HQ AFCESA/CEO - Air Force Civil Engineer Support Agency, Operations and Programs Support Division
HQ AFCESA/CEOA - Air Force Civil Engineer Support Agency, Operations and Programs Support Division, Engineer Support Branch
HTTPS - Hypertext Transfer Protocol Secure (combination of the Hypertext Transfer Protocol and a cryptographic protocol)
IA - information assurance
IAM - information assurance manager or management
IAO - information assurance officer
IAS - information assurance strategy
IAT - information assurance technical
IATO - interim authority to operate
IATT - interim authority to test
IAW - in accordance with
ICS - industrial control system
IDS - intrusion detection system
IOC - initial operating capability
IP - Internet Protocol
IPSec - Internet Protocol Security
IPT - integrated product team
IS - information system
ISM - industrial, scientific, and medical
IT - information technology
LAN - local area network
Ltr - letter
MAC - mission assurance category
MaC - media access control
MAJCOM - major command
MDIP - Modified DIACAP Implementation Plan
NIPRNet - Nonsecure Internet Protocol Router Network
NIST - National Institute of Standards and Technology
NIST SP - NIST Special Publication

Atch 2
(2 of 5)
Accreditation – A management decision by a senior agency official to authorize operation of a PIT-designated system based on the results of a certification analysis and other relevant considerations. The PIT DAA can grant system accreditation but cannot grant connection approval to the AF-GIG. Only the Air Force DAA may grant an ATC. The current Air Force DAA is AFSPC/A6.
Certification – A comprehensive analysis of the technical and non-technical aspects of an information system in its operational environment to determine compliance to stated security requirements and controls. The current Air Force CA is AFNIC.

Computing Environment – A computing environment has a server with multiple stations working from it. The stations can be standard computers, remote sensors, satellite feeds, etc.

Computer Network – The constituent element of an enclave responsible for connecting computing environments by providing short-haul data transport capabilities, such as LANs, or long-haul data transport capabilities, such as wide area and backbone networks.

Demilitarized Zone (DMZ) – A secure interface between systems or components of systems or a perimeter network that adds an extra layer of protection between internal and external networks by enforcing the internal network’s IA policy for external information exchange. A DMZ, also called a “screened subnet,” provides external, untrusted sources with restricted access to releasable information while shielding the internal network from outside attacks.

Enclave – A collection of computing environments connected by one or more internal networks under the control of a single approval authority and security policy, including personnel and physical security.

Global Information Grid (GIG) – The globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems. Non-GIG includes stand-alone, self contained, or embedded IT that is not, and will not be, connected to the enterprise network. (DODD 8000.01)

Information Assurance (IA) – Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

IA Control – An objective IA condition of integrity, availability, or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities that is expressed in a specified format, i.e., a control number, a control name, control text, and a control class. Specific management, personnel, operational, and technical controls are applied to each DOD information system to achieve and appropriate level of integrity, availability, and confidentiality in accordance with OMB Circular A-130. (DODI 8500.2)
Information System (IS) – A discrete set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. (Note: Includes AIS applications, enclaves, outsourced IT-based processes, and PITIs.)

Information Technology (IT) – Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This includes equipment used by the executive agency directly or used by a contractor under a contract with the executive agency, which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term “information technology” includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. Notwithstanding the preceding, the term “information technology” does not include any equipment that is required by a Federal contractor incidental to a Federal contract.

Mobile Code – Software modules obtained from remote systems, transferred across a network, and then downloaded and executed on local systems without explicit installation or execution by the recipient.

Privileged User – An authorized user who has access to system control, monitoring, or administration functions.

Type Accreditation – DODI 8510.01 defines type accreditation as “the official authorization to employ identical copies of a system in specified environments.” This form of C&A allows a single DIACAP package (i.e., System Identification Profile, DIACAP Implementation Plan, supporting documentation for certification, DIACAP Scorecard, and IT security POA&M [if required]) to be developed for an archetype (common) version of an IS that is deployed to multiple locations, along with a set of installation and configuration requirements or operational security needs, that will be assumed by the hosting location. AIS applications accreditations are type accreditations. Stand-alone IS and DMZ accreditations may also be type accreditations.
MEMORANDUM FOR AF/A7C

FROM: SAF/CIO A6
1800 Air Force Pentagon
Washington DC 20330-1800

SUBJECT: Appointment of Platform Information Technology (PIT) Designated Accrediting Authority (DAA)

1. In accordance with AF Policy Directive, Information Assurance Program, I hereby appoint the Air Force Deputy Civil Engineer (HQ USAF/A7C-2), the PIT DAA for all Civil Engineering Industrial Control systems (ICS) designated as PIT. AF/A7C has met the criteria, training, and certification requirements outlined in DoDI 8510.01E, Information Assurance, paragraph 4.25 and DoD 8570.1-M, Information Assurance Workforce Improvement Program, chapter 5. All Civil Engineering ICS categorized as PIT Interconnections (PITI) must obtain accreditation and connection approval from the Air Force Designated Accrediting Authority (AFSPC/A6) prior to connecting to the Air Force provisioned portion of the Global Information Grid (AF GiG).

2. The AF/A7C-2, as PIT DAA for Civil Engineering ICS, will maintain compliance with:

   a. DoD approved DAA training either through the DISA Online DAA Training Course

   b. Committee on National Security System Instruction 4012, National Information Assurance Training Standard for Senior System Managers

   c. Statutory requirements (FISMA, Clinger Cohen Act, Federal Information Processing Standards, etc.), DoD and Air Force information assurance policies.

3. SAF/CIO A6 maintains authority to revoke this appointment based on lack of due diligence, non-compliance with aforementioned policies, and other security related infractions. AF/A7C will provide semi-annual reports to SAF/A6O1 (af.infoassurance@pentagon.af.mil) providing status on all Civil Engineering PIT ICS accredited over the specified period. Direct any questions or comments to the SAF/CIO A6 point of contact, Ken Brodie, SAF/A6O1, DSN 425-1526, kenneth.brodie@pentagon.af.mil.

WILLIAM T. LORD, Lt Gen, USAF
Chief of Warfighting Integration and
Chief Information Officer

cc: AFSPC/CV/A6
AFNIC/EV
DISTRIBUTION LIST

SPECIAL INTEREST ORGANIZATIONS

Information Handling Services   (1)  Construction Criteria Database   (1)
15 Inverness Way East  
Englewood, CO 80150  
National Institute of Bldg Sciences 
Washington, DC 20005