DEPARTMENT OF THE NAVY
COMMANDER
NAVAL EDUCATION AND TRAINING COMMAND
250 DALLAS STREET
PENSACOLA, FLORIDA 32508-5220

NETCINST 5270.1C
N6
15 Nov 2022

NETC INSTRUCTION 5270.1C

From: Commander, Naval Education and Training Command

Subj: POLICY AND PROCEDURES FOR APPOINTMENT OF INFORMATION SYSTEMS SECURITY MANAGERS, INFORMATION SYSTEMS SECURITY OFFICERS, AND INFORMATION SYSTEMS SECURITY TRUSTED AGENTS

Ref: See Appendix A

1. Purpose. To establish policy and procedures, assign responsibilities, and provide direction for the identification and tracking of Naval Education and Training Command (NETC) Cyberspace Workforce positions and personnel assigned responsibilities as Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO), and Information Systems Security Trusted Agent (ISSTA).

2. Cancellation. NETCINST 5270.1B.

3. Discussion. This instruction provides guidance for assignment, appointment, and roles and responsibilities for designation of ISSMs, ISSOs, and ISSTAs for all commands within the NETC domain.

4. Action. Commands will review this manual and use it as guidance when appointing ISSMs, ISSOs, and ISSTAs. See Appendix A for references. Appendix B will be prepared based on the position the individual will be filling. In the event an individual's designation is rescinded, Appendix C will be utilized.

5. Records Management

a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned per the records disposition schedules located on the Department of the Navy Assistant for Administration, Directives and Records Management Division portal page at https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/AllItems.aspx.

b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact the local records manager.

6. Review and Effective Date. Per OPNAVINST 5215.17A, NETC will review this instruction annually around the anniversary of its issuance date to ensure applicability, currency, and consistency with Federal, Department of Defense, Secretary of the Navy, and Navy policy and statutory authority using OPNAV 5215/40 (Review of Instruction). This instruction will be in effect for 10 years, unless revised or cancelled in the interim, and will be reissued by the 10-year anniversary date if it is still required, unless it meets one of the exceptions in OPNAVINST 5215.17A, paragraph 9. Otherwise, if the instruction is no longer required, it will be processed for cancellation as soon as the need for cancellation is known following the guidance in OPNAV Manual 5215.1 of May 2016.

7. Forms. The following forms are available for download from the Department of the Navy Issuances website (https://www.secnav.navy.mil/doni/default.aspx):

a. SECNAV 5239/1 (Information System (IS) Privileged Access Agreement and Acknowledgment (PAA) or Responsibilities)

b. SECNAV 5500/1 (Electronic Spillage Action Form)

C. COLLINS, JR.
Chief of Staff

Releasability and distribution:
This instruction is cleared for public release and is available electronically on the NETC Public Web Site (www.netc.navy.mil), via the NETC Reference Library in DON TRACKER, or by e-mail at netc_directives@navy.mil.

NETCINST 5270.1C
15 Nov 2022

# GUIDANCE FOR

# INFORMATION SYSTEMS SECURITY MANAGER, INFORMATION SYSTEMS SECURITY OFFICER, AND INFORMATION SYSTEMS SECURITY TRUSTED AGENT APPOINTMENT AND DESIGNATION


**NAVAL EDUCATION AND TRAINING COMMAND**

**COMMAND INFORMATION OFFICE (N6)**

TABLE OF CONTENTS

# APPENDIX A

## REFERENCES

(a) DoD Directive 8140.01 of 5 October 2020

(b) DoD Instruction 8500.01 of 7 October 2019

(c) NETCINST 5239.1D

(d) CJCSI 6510.01F

(e) CJCSM 6510.01B

(f) DoD Instruction 8530.01 of 7 March 2016

(g) DoD Instruction 8510.01 of 19 July 2022

(h) DoD Instruction 8140.02 of 21 December 2021

(i) DoD Manual 8570.01, Information Assurance Workforce Improvement Program, of 19 December 2005

(j) DoD Manual 5200.02, Procedures for the DoD Personnel Security Program, of 3 April 2017

(k) DoD Manual 5200.01, Volumes 1 through 3, of 24 February 2012

(l) DoD 5200.08-R, Physical Security Program, of 19 October 2020

(m) 32 CFR 117

(n) SECNAVINST 5239.20A

(o) SECNAVINST 5239.3C

(p) SECNAVINST 3052.2

(q) SECNAVINST 5510.30C

(r) SECNAV M-5239.2

**GUIDANCE FOR
INFORMATION SYSTEMS SECURITY MANAGER (ISSM),
INFORMATION SYSTEMS SECURITY OFFICER (ISSO), AND
INFORMATION SYSTEMS SECURITY TRUSTED AGENT (ISSTA)
APPOINTMENT AND DESIGNATION**

1. OVERVIEW. Personnel assigned roles and responsibilities as NETC ISSM, ISSO, or ISSTA must be properly appointed or designated. This includes identification of roles and responsibilities necessary to perform assigned cybersecurity job tasks.

2. PURPOSE. To establish policy and procedures, assign responsibilities, and provide direction for the identification and tracking of Naval Education and Training Command (NETC) cyberspace workforce positions and personnel assigned responsibilities as ISSM, ISSO, or ISSTA per the authority in references (a) and (b). To define NETC-wide guidance on the assignment of ISSM, ISSO, and ISSTA responsibilities and provide the appropriate references for development of appointment or designation letters for those assigned responsibilities as NETC ISSM, ISSO, or ISSTA.

3. CONTROL OBJECTIVES. To establish cybersecurity (CS) methodology with NETC commands for appointing, designating, and defining roles for ISSM, ISSO, and ISSTA that are consistent with processes, strategies, and technologies references (a) through (r).

4. PREREQUISITE INSTRUCTION AND GUIDANCE. Reference (a) is the policy for CSWF Management. Reference (b) is the policy for CS. Reference (c) is the NETC policy for CS. Reference (d) provides joint policy and responsibilities for Information Assurance and Support to Computer Network Defense. Reference (e) describes the Department of Defense (DoD) Cyber Incident Handling Program. Reference (f) is the policy for the CS Activities Support to DoD Information Network Operations. Reference (g) is the policy for Risk Management Framework for DoD Systems. Reference (h) is the policy for support to DoD Information Network Operations. Reference (i) provides guidance for the Information Assurance Workforce Improvement Program. Reference (j) is the policy for Procedures for the DoD Personnel Security Program. Reference (k) is the policy for the DoD Information Security Program. Reference (l) is the policy for the Physical Security Program.

Reference (m) is the National Industrial Security Program Operating Manual. Reference (n) is the policy for the Department of the Navy (DON) Cyberspace Information Technology and CSWF Management and Qualification. Reference (o) is the policy for DON CS. Reference (p) established polices and responsibilities for the administration of cyberspace within the DON. Reference (q) is the policy for the DON Personnel Security Program. Reference (r) is the policy for DON Cyberspace Information Technology and CSWF Management and Qualification.

5. SCOPE. This guidance applies to all NETC commands and personnel appointed or designated to perform the roles and responsibilities of ISSM, ISSO, or ISSTA.

6. ROLES AND RESPONSIBILITIES. Table 1 delineates the primary roles and responsibilities of the individuals appointed or designated per this guidance. Additional roles and responsibilities for personnel appointed or designated as ISSM or ISSO are addressed in the references and NETC CS published guidance located on My Navy Portal at https://www.mnp.navy.mil/group/NETC-N6-Information-Management.

| Role | Current Organization | Responsibility |
|---|---|---|
| Echelon 2 CS Program Manager (CS-PM) | NETC Headquarters (HQ) | • Overall responsibility for NETC CS Program. |
| NETC ISSM or ISSO | NETC HQ | • Ensure all ISSM or ISSO and CS Trusted Agents are appointed or designated in writing.<br><br>• Ensure ISSM, ISSO, and ISSTA letters are complete and accurate for roles and responsibilties within their CS Area of Responsibilitiy (AOR) per references (a) through (r).<br><br>• Coordinate with the Naval Network Warfare Command Designated Approving Authority, the Global Network Operations Center, the Naval Cyber Defense Operations Command (NCDOC), the U.S. Fleet Cyber Command and U.S. TENTH Fleet, Navy Information Forces Command, and the DON as appropriate for CS issues. |

| | | |
|---|---|---|
| NETC Cyber Information Technology (IT) CSWF PM (Cyber IT and CSWF-PM) | NETC HQ | • ,Ensure ISSM, ISSO, and ISSTA qualifications are correctly identified for the billet to include up to three Defense CSWF work role code (DWRC) three-digit codes and meet proficiency levels (PL) per references (i), (l), (o), (p), and (r).<br><br>• Ensure ISSM, ISSO, and ISSTA have appropriate DWRCs and proficiency levels (PL) as required by Position Description (PD) "Conditions of Employment." Ensure ISSM, ISSO, ISSTA, DWRC, and PLs are properly annotated in both the PD and Total Workforce Management System (TWMS).<br><br>• Track and monitor ISSM, ISSO, and ISSTA qualifications for retention of ISSM, ISSO, and ISSTA authorities.<br><br>• Advise NETC CS-PM of personnel falling out of compliance.<br><br>• Maintain list of command ISSM and ISSO for NETC. |

| | | |
|---|---|---|
| Command ISSM | Echelon 3 and below | • Ensure receipt of appointment in writing by Commanding Officer or Officer In Charge.<br><br>• Ensure ISSOs and ISSTAs are appointed or designated in writing.<br><br>• Ensure compliance with references (a) through (r) and applicable Echelon 2 guidance.<br><br>• Coordinate with NETC and Command Cyber IT and CSWF-PM to ensure ISSM, ISSO, and ISSTA DWRCs and PLs are properly annotated in TWMS.<br><br>• Coordinate with NETC ISSM and Cyber IT and CSWF-PM for any changes in ISSM, ISSO, and ISSTA responsibilities.<br><br>• Submit ISSM and ISSO assignment letters and ISSM and ISSO termination letters to NETC ISSM.<br><br>• Provide contact information to the Immediate Superior in Command (ISIC) PM. |

| | | |
|---|---|---|
| Command Cyber IT and CSWF-PM | Echelon 3 | • Perform duties as described in NETC Cyber IT and CSWF-PM role respective to their command and appropriate NETC guidance.<br>• Maintain list of ISSMs, and ISSOs for the command.<br>• Ensure government civilian and military personnel are qualified per reference (r) and contract support CSWF personnel are qualified per reference (i). |

Table 1: Primary Roles and Responsibilities

7. GUIDANCE (ISSM, ISSO, AND ISSTA). NETC and echelon 3 subordinate commands shall reference this guidance and identify the specific responsibilities below in the command ISSM, ISSO, and ISSTA letters. All ISSM, ISSO, and ISSTA letters shall reference the paragraphs below for their assigned AOR. NETC ISSM positions are inherently governmental and shall be filled by DoD employees, military or civilian. Contractors may be assigned to ISSO or ISSTA positions only. All ISSO and ISSTA shall report to a properly designated Command ISSM at either the local command or the higher echelon. U.S. citizens must fill ISSM, ISSO, and ISSTA positions within NETC.

7.1. GENERAL REQUIREMENTS (ISSM AND ISSO). ISSM and ISSO shall satisfy all responsibilities as outlined in references (a) through (r). Implement, comply with, and maintain the NETC CS Program within assigned AOR. Provide security oversight for all Unit Identification Codes listed in ISSM and ISSO appointment letters including coordinating security measures such as analysis, periodic testing, evaluation, verification, accreditation, and review of Command IT assets.

7.2. APPROVALS (ISSM, ISSO, AND ISSTA). Ensure information ownership responsibilities are established for Command IT assets

to include accountability, access approvals, and special handling requirements. Approval may include:

a. (ISSM, ISSO, and ISSTA) CS approving authority for System Access Authorization Request-Navy.

b. (ISSM and ISSO) Privileged Access Agreement, per reference (r), is to be submitted to the command Cyber IT and CSWF-PM after ISSM, ISSO, and ISSTA signature.

c. (ISSM) Firewall Request.

d. (ISSM and ISSO) SECNAV 5500/1 (Electronic Spillage Action Form).

e. (ISSM and ISSO) Prepare the following and submit to NETC ISSM for approval as applicable:

(1) Assessment and Authorization, Security Plan, and Artifacts

(2) Privacy Impact Assessment

(3) Active Directory Organizational Unit Administrator Request

(4) Removable Media Device Exception (Legacy Non-classified Internet Protocol Router)

(5) Command Cyber Readiness Inspection and CS Inspection documentation

(6) (ISSM) Training Network Port Reconnect Requests

f. (ISSM and ISSO) Professional Certification and Licensing Voucher Requests are to be submitted to the Command Cyber IT and CSWF-PM for approval and routing to Navy Credentialing Opportunities Online.

g. (ISSM) Approve requests for ISSO and ISSTA designations and ensure ISSOs and ISSTAs are appointed in writing to include their assigned duties and responsibilities identified in reference (f).

h. (ISSM) Review and approve ISSOs necessary technical or management and CS training, education, and certifications required to carry out their respective duties.

i. (ISSM, ISSO, and ISSTA) Review and approve access requests in coordination with the Command Security Manager, ensuring command users and system support personnel have the required Background Investigation (BI), security clearance, authorization, and need-to-know and are indoctrinated on security practices before granting access to Command IT assets.

7.3. CYBER AWARENESS TRAINING (ISSM, ISSO, AND ISSTA). In coordination with the Command Training Manager or designated training representative, ensure authorized and privileged system users are provided initial and annual CS awareness training; and system administrator, management, and network security personnel are provided appropriate systems security training for their duties. Ensure CS awareness and appropriate systems security training are documented and tracked.

7.4. PRIVACY ACT TRAINING (ISSM, ISSO, AND ISSTA). In coordination with the Command Training Manager or designated training representative, ensure authorized and privileged system users are provided initial and annual Privacy Act (PA) or Personally Identifiable Information (PII) training each fiscal year. Ensure PA and PII training records are maintained in the designated DON CSWF tracking system.

7.5. RETENTION (ISSM, ISSO, AND ISSTA). Ensure CS-related artifacts addressed in paragraph 7.2 are maintained, traceable, and can be audited.

7.6. INFORMATION ASSURANCE VULNERABILITY MANAGEMENT (IAVM) (ISSM)

a. Review all IAV and CS tasks (i.e., Communication Tasking Orders and Navy Telecommunications Directives) and determine applicability to command IT assets and, when ISSOs are assigned, collaborate with ISSOs, or Technical Managers to develop an implementation plan and schedule. Create and document mitigation strategies and plans and submit to Command, ISIC, and NETC ISSM for review prior to submission into the Vulnerability Resource Asset Management System.

b. Monitor all IAV implementation and compliance for assets within AOR to ensure Command security baseline is established and maintained. Provide oversight and ensure reporting compliance (i.e., DON Vulnerability Remediation Asset Manager) is met and maintained as directed within the contents of the IA alerts, bulletins, technical notices, and guidance released by the DoD and DON. Report IAVM, Communications Tasking Order, and Naval Telecommunications Directive compliance status when directed by NETC ISSM.

7.7. CYBER IT AND CSWF RESPONSIBILITIES (ISSM). Command ISSM designated, in writing, shall perform PM duties per NETC approved Cyber IT and CSWF-PM appointment letters.

7.8. ASSESSMENT AND AUTHORIZATION (A&A) (ISSM AND ISSO). ISSM and ISSO with responsibility for CS oversight of IS, Platform Information Technology (PIT) environments, or Defense Business Systems shall ensure the development of artifacts (e.g., tables, drawings), review, endorsement, and maintenance of CS A&A artifacts, per reference (g), for initial accreditation decisions, annual reviews, and reauthorizations. This documentation and all modifications shall be maintained in the DON approved A&A repository, DON Enterprise Mission Assurance Support Service for unclassified and classified systems.

7.9. INCIDENT AND SPILLAGE HANDLING (ISSM AND ISSO)

a. Adhere to guidance and procedures to ensure security violations and incidents are properly reported to the Computer Network Defense Service Provider, NCDOC, and the DoD reporting chain, as required.

b. Ensure all computer incidents affecting your command are tracked, managed, investigated, resolved, and reported to NCDOC, NETC ISSM, and ISIC ISSM (i.e., Learning Center or echelon 3) per reference (e) and NETC Guidance for Incident Response.

7.10. AUDITING AND COMPLIANCE (ISSM, ISSO, AND ISSTA). ISSM and ISSO shall ensure compliance monitoring occurs, and review the results of such monitoring, notifying the NETC ISSM of significant CS vulnerabilities and threats (i.e., CAT I findings, open IAVs, large quantities of CAT II findings, etc.). ISSM, ISSO, and ISSTA shall ensure documents and training over which they have authority, per this guidance, are maintained so

that original and update records are traceable and can be audited.

7.11. CONFIGURATION MANAGEMENT (CM) (ISSM AND ISSO). The Command ISSM will serve as a member of the command CM board or delegate this responsibility to a properly appointed ISSO. Ensure procedures are developed and implemented per Command CM policies and practices for authorizing the use of software on IT assets and the introduction of new technologies that affect or impact existing security baselines. Assess security risk implications (i.e., threats to existing security baseline, mitigations) and coordinate and review with the Command ISSM and NETC ISSM. The Command ISSM will coordinate risk assessment and recommendations with NETC ISSM. NETC ISSM is the approval authority for accreditation boundary changes introduced by proposed technology.

8. ENFORCEMENT. Accountability requirements and enforcement metrics are specific to each guidance sub-process and are detailed in applicable Standard Operating Procedures (SOP).

9. TERMS. The paragraphs below provide definitions that are applicable to this guidance.

a. Certification. Recognition given to individuals who have met predetermined qualifications set by an agency of government, industry, or profession. Certification provides verification of individuals' knowledge and experience through evaluation and approval based on a set of standards for specific profession or occupations' functional job levels. Each certification is designed to stand on its own and represents a certified individual's mastery of a particular set of knowledge and skills. See also Office of Personnel Management Memorandum of 13 August 2008, Fact Sheet on Certification and Certificate Programs.

b. Cybersecurity. Measures taken for the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

c. CSWF. Personnel who secure, defend, and preserve data, networks, net-centric capabilities, and other designated systems by ensuring appropriate security controls and measures are in place, and taking internal defense actions. This includes access to system controls, monitoring, administration, and integration of CS into all aspects of engineering and acquisition of cyberspace capabilities.

d. Cyberspace Enabler Workforce. Personnel who perform work roles to support or facilitate the functions of cyber IT, CS, cyberspace effects, or intelligence workforce (cyberspace) work roles. This includes actions to support acquisition, training, and leadership activities.

e. Cyberspace Workforce. Personnel who build, secure, operate, defend, and protect DoD and U.S. cyberspace resources; conduct related intelligence activities; enable future operations; and project power in or through cyberspace. It is comprised of personnel assigned to the following workforce elements: IT, CS, cyberspace effects, intelligence workforce (cyberspace), portions of the intelligence workforces (non-cyber), and cyberspace enablers.

f. Cyber IT and CSWF PM. The Cyber IT and CSWF-PM will be responsible for the administration and management of the organization’s Cyber IT and CSWF Program. The Cyber IT and CSWF-PM is responsible for the reporting, database management, and overall effectiveness of the program at commands and subordinate units. Wherever possible, the Cyber IT and CSWF-PM role should be a primary duty. Only military or government civilian personnel may serve as a Cyber IT and CSWF-PM. In small commands, the functions of the Cyber IT and CSWF-PM may be performed by a higher level organization.

g. Information System (IS). A discreet set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See also Committee on National Security Systems Instruction No. 4009.

h. ISSM. Responsible for ensuring that all CS components have completed the appropriate evaluation and configuration processes prior to incorporation into or connection to an IS or PIT system.

i. ISSO. Assists the ISSMs in meeting their duties and responsibilities; implements and enforces all CS policies and procedures; ensures that all users have the requisite BI, security clearances, and access authorization; initiates protective or corrective measures when a CS incident or vulnerability is discovered; and ensures that all DoD IS CS-related documentation is current and accessible to properly authorized individuals.

j. IT Workforce. Personnel who design, build, configure, operate, and maintain IT, networks, and capabilities. This includes actions to prioritize, implement, evaluate, and dispose of IT as well as information resource management; and the management, storage, transmission, and display of data and information.

k. PIT. IT, both hardware and software, which is physically, part of, dedicated to, or essential in real time to the mission performance of special purpose systems.

l. PIT System. A collection of PIT within an identified boundary under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location.

m. Privileged User. A user who has roles that allow read, write, or change access to manage IT systems including system, network, or database administrators and security analysts who manage audit logs. IT privileged user roles are generic to all IT infrastructure, including transport, hosting environments, cybersecurity, and application deployment.

n. Privileged Access Agreement (PAA). Required for a privileged user, which is a user who is authorized, and therefore trusted, to perform security-relevant functions that ordinary users are not authorized to perform. PAA required for use is SECNAV Form 5239/1.

o. Work Role. Describes a distinct set of activities and attributes needed for the successful execution of work. A person may perform one or more work roles within their assigned position, billet, or contracted service requirement.

10. DELIVERABLES AND REPORTS. Deliverables and reports are specific to each guidance sub-process and are detailed in applicable SOPs.

APPENDIX B
SAMPLE DESIGNATION LETTER

**DEPARTMENT OF THE NAVY**
**COMMANDING OFFICER**
**[COMMAND NAME]**
**[COMMAND STREET ADDRESS]**
**[COMMAND CITY, STATE, ZIP CODE]**

5270
Ser N6/
DD MMM YY

From: Commanding Officer, Command Site Name Here
To: Name of Designee, Company Name when applicable

Subj: DESIGNATION AS INFORMATION SYSTEMS SECURITY (MANAGER, OFFICER, TRUSTED AGENT (choose appropriate designation)) FOR (COMMAND NAME AND LOCATION)

Ref: (a) NETCINST 5270.1C

1. Per reference (a), you are hereby designated as the Information Systems Security (Manager (ISSM), Officer (ISSO), Trusted Agent (ISSTA) choose appropriate designation) for (Command Name) in support of the (Command Name) command ISSM Cyber Security (CS) initiatives.

2. As a designated (ISSM, ISSO, ISSTA (choose appropriate designation)), you are responsible for support of the following Unit Identification Codes (UICs):

a. (UIC: PLA: )

b. (UIC: PLA: )

c. (UIC: PLA: )

3. Your duties as the (ISSM, ISSO, ISSTA (choose appropriate designation)) include, but are not limited to, those outlined in reference (a).

4. The command ISSM will notify the Naval Education Training Command (NETC) ISSM and NETC Cyber Information Technology and CS Work Force Program Manager when organization ISSM, ISSO, and ISSTA status changes, providing new point of contact

Subj: DESIGNATION AS INFORMATION SYSTEMS SECURITY (MANAGER, OFFICER, TRUSTED AGENT (choose appropriate designation)) FOR (COMMAND NAME AND LOCATION)

information. NETC will coordinate updates with commands external to NETC.

5. This designation is effective until rescinded in writing.

PRINTED NAME
By direction (if not signed by CO)

Copy to:
NETC ISSM
Echelon 3 ISSM (as applicable)
LC ISSM (as applicable)
[COMMAND] ISSM

APPENDIX C
SAMPLE DESIGNATION TERMINATION LETTER

**DEPARTMENT OF THE NAVY**
**COMMANDING OFFICER**
**[COMMAND NAME]**
**[COMMAND STREET ADDRESS]**
**[COMMAND CITY, STATE, ZIP CODE]**

5270
Ser N6/
DD MMM YY

From: Commanding Officer, Command Site Name Here
To: Name of Designee, Company Name when applicable

Subj: TERMINATION OF DESIGNATION AS INFORMATION SYSTEMS SECURITY (MANAGER, OFFICER, TRUSTED AGENT (choose appropriate designation)) FOR (COMMAND NAME AND LOCATION)

Ref: (a) NETCINST 5270.1C

1. Per reference (a), your designation as the Information Systems Security (Manager, Officer, Trusted Agent (choose appropriate designation)) for (Command Name) is hereby terminated.

PRINTED NAME
By direction (if not signed by CO)

Copy to:
NETC ISSM
Echelon 3 ISSM (as applicable)
LC ISSM (as applicable)
[COMMAND] ISSM