1. Everyone who needs access to EESOH-MIS has to authenticate through the AF Portal with a common access card. Are we duplicating work just for the sake of complying with DoD and Air Force security directives?

Common Access Card (CAC) issuance and the System Authorization Access Request to authorize access to an information system are mutually exclusive in that not all CAC holders are information system account holders. According to the DoD 8500.01E Information Assurance, “Access to all DoD information systems shall be based on a demonstrated Need-to-Know, and granted in accordance with applicable laws and DoD 5200.2-R (reference (n)) for background investigations, special access and IT position designations and requirements.” The Need-to-Know Determination is a decision made by an authorized holder of official information that a prospective recipient requires access to specific official information to carry out official duties (reference (i)). The DD Form 2875 is a DoD approved System Authorization Access Request Form that verifies/validates users’ Need-to-Know/authorized access.

2. Is SAAR DD 2875 requirement just for ESSOH-MIS or do all Air Force systems require a DD Form 2875?

Users of any Air Force system must complete a SAAR DD 2875 for each system to comply with DoD Directive 8500.01E, Air Forces Systems Security Information (AFSSI) 8520, and the SAF/CIO A6 Memo, which states that system users must have a Need-to-Know for the information contained in the information system before access is granted. ESSOH-MIS uses a tailored DD 2875 to validate users’ Need-to-Know access.

3. Who/What is the Functional Appointee?

The Functional Appointee is responsible for approving access to EESOH-MIS and retains the SAAR DD Form 2875 for filing and auditing purposes. The Functional Appointee is appointed in writing and communicated to the appropriate HQ Forward Operating Agencies (FOAs), MAJCOM A7s, National Guard Base/A7A and installation level. Refer to EESOH-MIS Functional Appointee Matrix (Question 2) to determine the appropriate Functional Appointee.

4. What is the Functional Appointee Matrix?
The Functional Appointee Matrix below determines the appropriate Functional Appointee responsible for approving EESOH-MIS access and retaining the SAAR for filing and auditing purposes. First determine the type of EESOH-MIS user, then the user’s functional area (i.e. HazMat, HazWaste or Cleanup). Your supervisor should be able to tell you exactly who the Functional Appointee is and his/her phone number from the SAAR POC List posted on the EESOH-MIS support portal.

**NOTE:** If any user has the Cleanup function along with HazMat or HazWaste functions, the Cleanup takes precedence for SAAR management. For example, if a Cleanup non-National Guard Bureau (NGB) user at base “X” is doing Cleanup and HazMat in EESOH-MIS, then AFCEE/ERD SAAR POC manages the user’s SAAR.

<table>
<thead>
<tr>
<th>Type User</th>
<th>EESOH-MIS User Functional Areas</th>
<th>Functional Appointee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation User to include installation level contractors</td>
<td>HazMat</td>
<td>HazWaste</td>
</tr>
<tr>
<td>Installation SAAR POC</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>National Guard Bureau (NGB) - MAJCOM staff User</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Non NGB - MAJCOM staff User</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Non NGB - Cleanup User at any location/level</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Air Staff and SAF Offices</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>MAJCOM/FOA level Support Contractors</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>EESOH-MIS Program Office to include PO contractors</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Table 1  EESOH-MIS Functional Appointee Matrix
5. **What if I already completed a DD Form 2875 with previous instructions?**

Since DoD and Air Force security directives change over time, sometimes it is necessary to verify that completed security forms are still applicable. However, any previously finalized EESOH-MIS DD Form 2875 does NOT have to be redone. Those users who submitted their DD Form 2875 prior to January 2011 need to sign the Rules of Behavior Acknowledgement form which can be found on the EESOH-MIS support website. It contains the same information needed in Block 27 of an updated Form 2875 which contains the paragraph acknowledging the user understands the Rules of Behavior. This will ensure that all users are in compliance with AF 33-200, AFSSI 8520, and the EESOH-MIS System Support Plan.

6. **How will I know my Form has been successfully processed?**

The Functional Appointee will notify prospective users when account is active.

7. **Why is the DD Form 2875 maintained with the local Functional Appointee?**

There are four reasons:

   a. Local Functional Appointee has the information and visibility on who is approved to access EESOH-MIS and what roles they require.

   b. They are notified when a user transfers, retire, separates, or is terminated and coordinates inactivating/disabling user accounts with the EESOH-MIS Help Desk.

   c. The EESOH-MIS user access is required to be revalidated on an annual basis and the local Functional Appointee has the knowledge to be able to do the validation.

   d. For auditing purposes, all DD Form 2875s must be locally accessible.

8. **How long will this DD Form 2875 be valid?**

The form is valid indefinitely; however, there is an annual account review requirement by the Functional Appointee. When/if a user no longer needs access to EESOH-MIS the DD Form 2875 is to be retained for auditing purposes for one year after inactivating the account.

9. **What is the annual revalidation of DD Form 2875?**

Air Force System Security Instruction (AFSSI) 8520 requires that DD Form 2875s are reviewed annually to validate whether users continue to need access to the information systems for which they are authorized. The Functional Appointee is responsible for performing the review which consists of contacting the user and revalidate user account and assigned installation and roles, per
10. **Who can I call for assistance in completing my Form DD Form 2875?**

Contact your supervisor or Functional Appointee. If either of them needs further guidance, they can obtain assistance from the EESOH-MIS Help Desk at 866-488-4069.

11. **Can I use electronic signatures?**

Yes.

12. **Will AF-EMIS users have to comply with the EESOH-MIS version of the DD Form 2875?**

The DD Form 2875 was tailored for EESOH-MIS access and only applies to EESOH-MIS user accounts. AF-EMIS is being sun downed and migrated over to EESOH-MIS. AF-EMIS users migrating over to EESOH-MIS will need to fill out the tailored DD Form 2875 to validate their Need-to-Know access within EESOH-MIS.

13. **If any of the information on the Form changes, like the supervisor, is another Form required?**

Only if the information changed affects the user’s authorized access to EESOH-MIS, e.g. lost appropriate security clearance, Need-to-Know changes, etc. However, if the user transfers to another location, the user's account access must be disabled and then a new DD Form 2875 prepared at the gaining location if access is still required there.

14. **Since EESOH-MIS is unclassified, why are we asking for the clearance level and type of investigation?**

You're correct that EESOH-MIS is not a classified system and therefore the clearance level (28b of the DD Form 2875) is not a mandatory fill box. However, AFI 33-501 for Personal Security Program Management requires security managers to validate the background investigation information tied to MAC III (unclassified) systems. Investigative information is found in the Joint Personal Adjudication System (JPAS) by the security manager. The clearance level information is also conveniently displayed on the same page as the background investigation and is usually annotated in Block 28b along with the type of investigation. At a minimum, EESOH-MIS users who are military personnel require a National Agency Check (NAC), civilian personnel require a National Agency Check plus written Inquiries (NACI), and contractors or consultants require a NAC.

15. **This Form is asking for the Information Assurance (IA) training date. Do we have to keep track of our refreshers as well or is this a onetime requirement?**
Per Federal Information Security Management Act (FISMA), DOD information assurance awareness is required for all individuals (Military, Civilian, and Contractors) before being granted access to DoD Information Technology (IT) systems. Annual recurring IA awareness training is required to retain access to DoD IT systems. The DD Form 2875 requires the date of IA training at the time the form is filled out. A new DD Form 2875 is not required each time the annual IA training is taken.

16. EESOH-MIS Functional Appointees are required to maintain the Form for one year past the termination of a user’s access to EESOH-MIS. Is this just for our base or if they go to another base where they may have access, will we need to maintain it for longer or forward it to their gaining base?

Do not forward forms. The original DD Form 2875 with original signatures in Part I, II, and III must be maintained on file with the local Functional Appointee for one year after termination of user’s access to EESOH-MIS. If the user transfers to another location, user’s account access should be disabled and then a new DD Form 2875 prepared at the gaining location if access is required there.

17. Does anyone audit the files maintained by the Functional Appointee?

Yes, the Air Force Audit Agency can/will audit the account management process and access controls using the Federal Information System Control Audit Manual (FISCAM) as the measuring guidance.

18. If someone transfers to another base doing the same function and maintains the same Need-to-Know level but the only information change is supervisor and user location information, would they need to complete another DD Form 2875 at the new gaining location or just forward a copy of the DD Form 2875 to the gaining unit?

Short answer is, complete a new DD Form 2875 at gaining location, and do not forward old forms. There are several reasons for this action. A person with access at one base may not necessarily have the same access at another base. The intention may be for the person to have the same function/role but upon arrival finds that the situation has changed and the person has been assigned a different function. Also, the need to know depends on supervisor approval. The new supervisor may not grant the same level of access and should have the right to determine the user's revised access rights. Also, how often does it occur that a losing supervisor knows exactly what the user's rights will be at a gaining base? What could occur is that a user has rights w and x at the old location but at the new base needs rights x, y, and z for the same job. Most likely the new rights will be granted without deleting right w. The result is a user with excessive rights and system vulnerability. Therefore, if the user transfers to another location, user’s account access should be disabled and then a new Form prepared at the gaining location if access is required there.
19. If a security manager waiver is not possible, is there a particular security manager who must sign the Form, e.g. the user’s organization security manager?

Any local security manager with Joint Personnel Adjudication System (JPAS) access to validate background investigation type and date can sign the DD Form 2875. This validation check provides the latest security status at the time of authorized access.

20. I know there are personnel from HQ and contractors who have access to EESOH-MIS and can see/manipulate our data. Am I required to have a copy of their DD Form 2875 as well?

The local Functional Appointee is only responsible to maintain the DD Form 2875 for EESOH-MIS users that physically reside at their installations or geographically separated units under that installation. This applies to contractors also residing at the installation.

21. Are there any issues with the contractors signing the DD Form 2875 as the Functional Appointee?

No issues. They may be appointed by the appropriate MAJCOM POC the same as an active duty or civil servant Functional Appointee.

22. With regard to MAJCOM POCs and support contractors that require access to multiple installations, is a separate DD Form 2875 required for each installation or is one sufficient? Who should be the Functional Appointee for these access levels?

Only one DD Form 2875 is required. Refer to the Functional Appointee Matrix in question #2 for determining the Functional Appointee.

23. What guidance dictates that access authorizations be based on Need-to-Know and should be documented on standard Forms and maintained on file?

Below are key DoD and Air Force policies and instructions along with applicable sections that apply to access authorization.

**CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION**

* CJCSI 6510.01E current as of 12 Aug 2008

8. Information and Information System Access. Access to DOD information systems is a revocable privilege and will be granted to individuals based on Need-to-Know and IAW DODI 8500.2 (reference e), NTISSP No. 200 (reference u), and DOD 5200.2-R (reference v) for clearance, special access, and IT designation and implementation of system user access requirements and responsibilities.

AC-3.1 User accounts are appropriately controlled (Page 223)

Owners should periodically review access authorization listings and determine whether they remain appropriate. Access authorizations should be documented on standard Forms and maintained on file. Listings of authorized users and their specific access needs and any modifications should be approved by an appropriate senior manager and directly communicated in writing by the resource owner to the security management function. A Formal process for transmitting these authorizations, including the use of standardized access request Forms, should be established to reduce the risk of mishandling, alterations, and misunderstandings.

Critical Element AC-2. Implement effective identification and authentication Mechanisms (Page 214)

At the entity-wide level, information systems accounts need to be managed to effectively control user accounts and identify and authenticate users. Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. Resource owners should identify authorized users of the information system and specify access rights. Access to the information system should be granted based on a valid need to know that is determined by assigned official duties and should also consider proper segregation of duties. The entity should require proper identification for requests to establish information system accounts and approve all such requests.

http://www.gao.gov/new.items/d09232g.pdf

DEPARTMENT OF DEFENSE DIRECTIVE 8500.01E INFORMATION ASSURANCE
8500.01E certified current as of Apr 23, 2007

4.8. Access to all DoD information systems shall be based on a demonstrated Need-to-Know, and granted in accordance with applicable laws and DoD 5200.2-R (reference (n)) for background investigations, special access and IT position designations and requirements. An appropriate security clearance and non-disclosure agreement are also required for access to classified information in accordance with DoD 5200.1-R (reference (o)).

E2.1.28. Need-to-Know. Necessity for access to, or knowledge or possession of, specific official DoD information required to carry out official duties (reference (i) modified).

E2.1.29. Need-to-Know Determination. Decision made by an authorized holder of official information that a prospective recipient requires access to specific official information to
carry out official duties (reference (i)).

AIR FORCES SYSTEMS SECURITY INFORMATION (AFSSI) 8520
IDENTIFICATION AND AUTHENTICATION 18 Jun 2009

5.2.1. Organizations will make sure a method is in place to authenticate user requests for systems and network access before enabling account access.

SAF/CIO A6 Memo
18 May 2010

MEMORANDUM FOR DISTRIBUTION C
FROM: SAF/CIO A6
1800 Air Force Pentagon
Washington, DC 20330

SUBJECT: Access Controls for Air Force Information Systems

1. The Air Force Audit Agency recently completed Project F2009-FB2000-0058.000, Financial System Access Controls. Although the audit focused on financial systems, it clearly identified systemic weaknesses in authentication, access, authorization, and account management security practices across all functional systems. This memorandum serves to heighten the awareness, stress due diligence and policy compliance of system owners, administrators, and information assurance managers in the implementation of access controls for their respective systems.

2. Specifically, compliance with Air Force Systems Security Instruction (AFSSI), 8520, Identification and Authentication, is mandatory and provides the overarching policy to ensure secure and best practice account management activities are conducted. I strongly encourage all system owners leveraging current technologies (Active Directory, Group Policies (GPOs), password enforcement tools, etc.) to enforce access control policies. In addition, we must ensure accounts are managed properly and with emphasis on creation, suspension, and removal in a timely manner to ensure vulnerabilities associated with dormant accounts are satisfactorily mitigated.

3. The vulnerabilities associated with access controls and account management, if not mitigated, leave our information systems and their data at high risk, susceptible to loss, misuse, unauthorized access, and unauthorized modification. I highly encourage your support in helping us secure our systems and information to ensure mission assurance for our warfighters.
4. The SAF/CIO A6 point of contact is Mr. Kenneth Brodie, SAF/A6NI, DSN 426-7557, kenneth.brodie@pentagon.af.mil.

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

EESOH-MIS SYSTEM SECURITY PLAN Version 1.3.0

1.2 Method of Access Control
A prospective EESOH-MIS user is required to obtain a DoD Local Area Network (LAN) account and DoD Common Access Card (CAC), along with subsequent access to the Air Force Portal as a pre-requisite for EESOH-MIS access. The user must then complete a SAAR DD Form 2875, to document that he/she has a valid Need-to-Know for the information contained in the information system before access is granted. Need-to-Know determination is the decision made by an authorized holder of official information that a prospective recipient requires access to specific official information to carry out official duties (reference (i)). Ref: Department of Defense Directive 8500.01E Information Assurance. The user’s supervisor is responsible for verifying Need-to-Know and determining access requirements. User access is role-based and restricted based on Need-to-Know and least-privilege principles per installation. The DD Form 2875 is coordinated through the user’s management and security channels for approval and then forwarded to the appropriate functional appointee for approving EESOH-MIS access and retained for filing and auditing purposes. The type of EESOH-MIS user and their functional area (i.e. HazMat, HazWaste and Clean-Up) determines the appropriate functional appointee (Refer to the EESOH-MIS Functional Appointee Matrix in the Account Management Policy. After the appropriate functional appointee validates the DD Form 2875, he/she notifies the EESOH-MIS Helpdesk, through a “digitally signed” e-mail, so that the user account can be created and roles assigned per installation based on the validated DD Form 2875. The digitally signed e-mail ensures the request is from a “verified” functional appointee through non-repudiation. The EESOH-MIS accounts are established by the EESOH-MIS Helpdesk. The EESOH-MIS Helpdesk will notify the functional appointee once the account is activated, who will in turn notify the prospective user. The user can then log into their EESOH-MIS account using their CAC. The account access procedure is summarized in the flowchart (Figure 1)
Figure 1 EESOH-MIS Access Control Flowchart