

<b>AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT</b>			1. CONTRACT ID CODE	PAGE OF PAGES 1   15
2. AMENDMENT/MODIFICATION NO. 02	3. EFFECTIVE DATE 19 Sep 08	4. REQUISITION/PURCHASE REQ. NO. SEE SCHEDULE	5. PROJECT NO. (If applicable)	
6. ISSUED BY 92nd Contracting Sq/LGCC 110 W Ent St., Suite 200 Fairchild AFB, WA 99011 POC: Ed Campbell	CODE	7. ADMINISTERED BY (If other than Item 6) SAME AS BLOCK 6	CODE	
8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code)  <b>TO ALL PROSPECTIVE OFFERORS</b>			(√)	9A. AMENDMENT OF SOLICITATION NO.
				9B. DATED (SEE ITEM 11)
			X	10A. MODIFICATION OF CONTRACT/ORDER NO. FA4620-08-Q-A081
				10B. DATED (SEE ITEM 13)
CODE	FACILITY CODE			

## 11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

- The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers  is extended,  is not extended. Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods:
- (a) By completing Items 8 and 15, and returning \_\_\_\_\_ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

## 13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACT/ORDERS, IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

- (√) A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
- B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
- C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
- D. OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor  is not,  is required to sign this document and return 1 copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

**This amendment pertains to EMCS Phase 3 at Fairchild AFB.**

The purpose of Amendment 2 is to identify the location of the main electrical panel in buildings 2005 and 2007. The main electrical service panel is located in Rm 120 on the first floor. The room number is the same for both bldg 2005 and 2007. In addition answers to questions from the site visit are attached.

A signed copy of this amendment must be returned with the contractor's proposal.

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10 A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print)		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)	
15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA	16C. DATE SIGNED
_____ (Signature of person authorized to sign)		BY _____ (Signature of Contracting Officer)	

19 Sep 2008

Amendment 2 answers to questions asked during the site visit.

1. Will the process to obtain an Interim Authority to Operate/Certificate to Operate (IATO/CTO) last the duration of the project?

Answer: The government does not know how long it will take the contractor with the successful proposal to obtain an IATO/CTO. It is the government's expectation that the process will be started shortly after award and will be successful within one year, not including government delays. Government delays will be determined by the Contracting Officer and will include delays for processing and the like.

2. Who is the first point of contact for obtaining an IATO/CTO?

Answer: Prior to award, all questions regarding IATO/CTO should be directed to the Contracting Officer. After award, the first point of contact to gain an IATO/CTO is the Communications Squadron Network Administration. A specific POC will be provided to the successful contractor at time of award.

3. What is the process for obtaining an IATO/CTO?

Answer: The current checklists used to gain an IATO/CTO are attached to this amendment. These will be used to establish an EITDR account.

4. Will EMCS Phase 3A, 3B, and 5A run concurrently?

Answer: Yes

5. What is included in the training cost estimate?

Answer: The estimate should include cost of the training and any lodging and per diem associated with the training.

6. What does the government mean by salient characteristics?

Answer: Salient characteristics are the physical, functional, and performance characteristics necessary to meet the government requirement.

7. Is the government looking for a specific brand?

Answer: No, any brand that meets the salient characteristics is acceptable.

8. What is the government expecting as proof of salient characteristics?

Answer: The government is expecting sufficient documentation, such as cut sheets, so that it can determine that the particular end item is suitable for the government's purpose.

9. Do the meters need to meet salient characteristics?

Answer: Yes, all components scheduled to be installed under a particular EMCS phase must meet (or exceed) the salient characteristics identified for that component.

10. What do the sensors for the gas meters measure?

Answer: The technical description and controller system specifications indicate what is measured. In this instance accumulated volume is what needs to be measured.

11. Can the contractor use existing conduit for the wire run to the old part of the Flight Simulator?

Answer: Yes you can use existing conduit for this wire run.

12. Does the number of inputs and outputs have to exactly match the solicitation requirements?

Answer: No they may meet or exceed as stated in the project description.

## Instructions on Completing the DD2875 (dated April 2005) for EITDR

The DD Form 2875 can now be signed digitally. Forms need to be completed in their entirety, if unsure of an answer to one of the following, please email [ossw.wpeitdr@wpafb.af.mil](mailto:ossw.wpeitdr@wpafb.af.mil) your question(s) or call DSN 787-8422.

To begin the process you should save the PDF file to your computer.

**Do not save your personal information on the EITDR CoP.**

### Type Of Request:

1. Select the type of request: initial, modification or deletion
2. Place your **AF PORTAL ID** in the User ID field (PORTAL ACCOUNT MUST BE OBTAINED PRIOR TO RECEIVING AN EITDR ACCOUNT)
3. System Name: EITDR
4. Location: DECC-D Dayton

### Part I: (required fields)

1. Name
2. Full SSN#
3. Organization
4. Office Symbol/Department
5. Phone (DSN)
6. Official Email Address
7. Job Title and Grade/Rank
8. Official Mailing Address
9. Citizenship
10. Designation of Person; Military, Civilian or Contractor
11. Signature of Requestor
12. Date signed

Note: If signing digitally, forward the electronic file to your supervisor for further processing.

### Part II: (required fields)

13. Justification For Access; Annotate the need for access (READ-ONLY ACCOUNTS WILL BE GRANTED BY THE EITDR ADMIN. FURTHER EDITING PERMISSIONS ASSIGNED BY THE PFM/POCs)
14. Check "Authorized"
15. Check "Unclassified"
16. Check the box
- 16a. For contractors, provide contract and company information as indicated.
17. Supervisor's Name
18. Supervisor's Signature (Government sponsor for Contractors)
19. Date of signature
20. Supervisor's Org
- 20a. Supervisor's Email Address
- 20b. Supervisor's DSN

### Notes:

1. If signing digitally, forward the electronic file to the security manager.
2. EITDR Help Desk personnel will complete blocks 21 - 25

Part III: (required fields) Note: The information pertaining to Part III is best referenced by your Security Manager

- 28. Type of Investigation (MOST RECENT FROM “ADJUDICATION SUMMARY”)
- 28a. Date of Investigation (DATE INVESTIGATION CLOSED FROM “ADJUDICATION SUMMARY” / CAN NOT BE MORE THAN 10 YEARS OLD)
- 28b. Clearance Level (FROM “ADJUDICATION SUMMARY” / MINIMUM REQUIRED “FAVORABLE NAC”)
- 29. Verified By
- 30. Security Manager Phone #
- 31. Security Manager Signature
- 32. Date of signature

Note: If signing digitally, send the completed file to the original requestor.

Part IV: (not required)

SUBMITTAL:

Prior to submitting the form please ensure:

1. YOU MUST PROVIDE YOUR AIR FORCE PORTAL LOGON ID.
2. ENSURE ALL REQUIRED SIGNATURES ARE IN PLACE.
3. THE SECURITY INVESTIGATION DATE IS NOT OUT OF SCOPE

Once completed in it’s entirety, the form can be sent to the EITDR Help Desk. If you have digital signatures just forward the completed file. If you have “ink” signatures, scan the document as a PDF file and send via email. The EITDR Help Desk e-mail is: [ossw.wpeitdr@wpafb.af.mil](mailto:ossw.wpeitdr@wpafb.af.mil) The digital signature file is the preferred method for submitting applications since your SSN is on the form.

Note: Signatures must be of all the same type. Either all digital or all ink. If digital signatures are used, the form must be received so we can view the digital signature certificates.

If any fields are not complete or all necessary signatures were not obtained, the form will be destroyed and the requestor will be asked to resubmit once the deficient area(s) are corrected.

You will receive an e-mail notification once the account has been established. Typical response time is 2-5 business days.

## SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

### PRIVACY ACT STATEMENT

**AUTHORITY:** Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.  
**PRINCIPAL PURPOSE:** To record names, signatures, and Social Security Numbers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.  
**ROUTINE USES:** None.  
**DISCLOSURE:** Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

<b>TYPE OF REQUEST</b> <input checked="" type="checkbox"/> INITIAL <input type="checkbox"/> MODIFICATION <input type="checkbox"/> DEACTIVATE <input type="checkbox"/> USER ID	<b>DATE (YYYYMMDD)</b> _____
--	---------------------------------

<b>SYSTEM NAME (Platform or Applications)</b> EITDR	<b>LOCATION (Physical Location of System)</b> _____
--	--

**PART I (To be completed by Requestor)**

1. NAME (Last, First, Middle Initial)	2. SOCIAL SECURITY NUMBER
3. ORGANIZATION 92 Comm Squadron	4. OFFICE SYMBOL/DEPARTMENT
5. PHONE (DSN or Commercial)	6. OFFICIAL E-MAIL ADDRESS
7. JOB TITLE AND GRADE/RANK	8. OFFICIAL MAILING ADDRESS
9. CITIZENSHIP <input checked="" type="checkbox"/> US <input type="checkbox"/> FN <input type="checkbox"/> OTHER	10. DESIGNATION OF PERSON <input checked="" type="checkbox"/> MILITARY <input type="checkbox"/> CIVILIAN <input type="checkbox"/> CONTRACTOR

### USER AGREEMENT

I accept the responsibility for the information and DoD system to which I am granted access and will not exceed my authorized level of system access. I understand that my access may be revoked or terminated for non-compliance with DoD security policies. I accept responsibility to safeguard the information contained in these systems from unauthorized or inadvertent modification, disclosure, destruction, and use. I understand and accept that my use of the system may be monitored as part of managing the system, protecting against unauthorized access and verifying security problems. I agree to notify the appropriate organization that issued my account(s) when access is no longer required.

**IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (Complete as required for user or functional level access.)**

I have completed Annual Information Awareness Training.      **DATE (YYYYMMDD)** \_\_\_\_\_

11. USER SIGNATURE	12. DATE (YYYYMMDD)
--------------------	---------------------

**PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR (If individual is a contractor - provide company name, contract number, and date of contract expiration in Block 16.)**

13. JUSTIFICATION FOR ACCESS  
 To accomplish certification and accreditation process.

14. TYPE OF ACCESS REQUIRED:  
 AUTHORIZED     PRIVILEGED

15. USER REQUIRES ACCESS TO:     UNCLASSIFIED     CLASSIFIED (Specify category)  
 OTHER \_\_\_\_\_

16. VERIFICATION OF NEED TO KNOW I certify that this user requires access as requested. <input type="checkbox"/>	16a. ACCESS EXPIRATION DATE (Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 27 if needed.) _____
---	---

17. SUPERVISOR'S NAME (Print Name) St	18. SUPERVISOR'S SIGNATURE	19. DATE (YYYYMMDD)
--	----------------------------	---------------------

20. SUPERVISOR'S ORGANIZATION/DEPARTMENT	20a. SUPERVISOR'S E-MAIL ADDRESS	20b. PHONE NUMBER
--	----------------------------------	-------------------

21. SIGNATURE OF INFORMATION OWNER/OPR	21a. PHONE NUMBER	21b. DATE (YYYYMMDD)
--	-------------------	----------------------

22. SIGNATURE OF IAO OR APPOINTEE	23. ORGANIZATION/DEPARTMENT	24. PHONE NUMBER	25. DATE (YYYYMMDD)
-----------------------------------	-----------------------------	------------------	---------------------

26a. NAME (Last, First, Middle Initial)	26b. SOCIAL SECURITY NUMBER
---	-----------------------------

27. OPTIONAL INFORMATION (Additional information)

**PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION**

28. TYPE OF INVESTIGATION	28a. DATE OF INVESTIGATION (YYYYMMDD)
28b. CLEARANCE LEVEL	28c. IT LEVEL DESIGNATION <input type="checkbox"/> LEVEL I <input type="checkbox"/> LEVEL II <input type="checkbox"/> LEVEL III
29. VERIFIED BY (Print name)	30. SECURITY MANAGER TELEPHONE NUMBER
31. SECURITY MANAGER SIGNATURE	
32. DATE (YYYYMMDD)	

**PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION**

TITLE:	SYSTEM	ACCOUNT CODE
	DOMAIN	
	SERVER	
	APPLICATION	
	DIRECTORIES	
	FILES	
	DATASETS	
DATE PROCESSED (YYYYMMDD)	PROCESSED BY (Print name and sign)	DATE (YYYYMMDD)
DATE REVALIDATED (YYYYMMDD)	REVALIDATED BY (Print name and sign)	DATE (YYYYMMDD)

## INSTRUCTIONS

The prescribing document is as issued by using DoD Component.

**A. PART I:** The following information is provided by the user when establishing or modifying their USER ID.

- (1) Name. The last name, first name, and middle initial of the user.
- (2) Social Security Number. The social security number of user.
- (3) Organization. The user's current organization (i.e. DISA, SDI, DoD and government agency or commercial firm).
- (4) Office Symbol/Department. The office symbol within the current organization (i.e. SDI).
- (5) Telephone Number/DSN. The Defense Switching Network (DSN) phone number of the user. If DSN is unavailable, indicate commercial number.
- (6) Official E-mail Address. The user's official e-mail address.
- (7) Job Title/Grade/Rank. The civilian job title (Example: Systems Analyst, GS-14, Pay Clerk, GS-5)/military rank (COL, United States Army, CMSgt, USAF) or "CONT" if user is a contractor.
- (8) Official Mailing Address. The user's official mailing address.
- (9) Citizenship (US, Foreign National, or Other).
- (10) Designation of Person (Military, Civilian, Contractor).

IA Training and Awareness Certification Requirements. User must indicate if he/she has completed the Annual Information Awareness Training and the date.

(11) User's Signature. User must sign the DD Form 2875 with the understanding that they are responsible and accountable for their password and access to the system(s).

(12) Date. The date that the user signs the form.

**B. PART II:** The information below requires the endorsement from the user's Supervisor or the Government Sponsor.

(13) Justification for Access. A brief statement is required to justify establishment of an initial USER ID. Provide appropriate information if the USER ID or access to the current USER ID is modified.

(14) Type of Access Required: Place an "X" in the appropriate box. (Authorized - Individual with normal access. Privileged - Those with privilege to amend or change system configuration, parameters, or settings.)

(15) User Requires Access To: Place an "X" in the appropriate box. Specify category.

(16) Verification of Need to Know. To verify that the user requires access as requested.

(16a) Expiration Date for Access. The user must specify expiration date if less than 1 year.

(17) Supervisor's Name (Print Name). The supervisor or representative prints his/her name to indicate that the above information has been verified and that access is required.

(18) Supervisor's Signature. Supervisor's signature is required by the endorser or his/her representative.

(19) Date. Date supervisor signs the form.

(20) Supervisor's Organization/Department. Supervisor's organization and department.

(20a) E-mail Address. Supervisor's e-mail address.

(20b) Phone Number. Supervisor's telephone number.

(21) Signature of Information Owner/OPR. Signature of the functional appointee responsible for approving access to the system being requested.

(21a) Phone Number. Functional appointee telephone number.

(21b) Date. The date the functional appointee signs the DD Form 2875.

(22) Signature of Information Assurance Officer (IAO) or Appointee. Signature of the IAO or Appointee of the office responsible for approving access to the system being requested.

(23) Organization/Department. IAO's organization and department.

(24) Phone Number. IAO's telephone number.

(25) Date. The date IAO signs the DD Form 2875.

(27) Optional Information. This item is intended to add additional information, as required.

**C. PART III:** Certification of Background Investigation or Clearance.

(28) Type of Investigation. The user's last type of background investigation (i.e., NAC, NACI, or SSBI).

(28a) Date of Investigation. Date of last investigation.

(28b) Clearance Level. The user's current security clearance level (Secret or Top Secret).

(28c) IT Level Designation. The user's IT designation (Level I, Level II, or Level III).

(29) Verified By. The Security Manager or representative prints his/her name to indicate that the above clearance and investigation information has been verified.

(30) Security Manager Telephone Number. The telephone number of the Security Manager or his/her representative.

(31) Security Manager Signature. The Security Manager or his/her representative indicates that the above clearance and investigation information has been verified.

(32) Date. The date that the form was signed by the Security Manager or his/her representative.

**D. PART IV:** This information is site specific and can be customized by either the DoD, functional activity, or the customer with approval of the DoD. This information will specifically identify the access required by the user.

**E. DISPOSITION OF FORM:**

**TRANSMISSION:** Form may be electronically transmitted, faxed, or mailed. Adding a password to this form makes it a minimum of "FOR OFFICIAL USE ONLY" and must be protected as such.

**FILING:** Original SAAR, with original signatures in Parts I, II, and III, must be maintained on file for one year after termination of user's account. File may be maintained by the DoD or by the Customer's IAO. Recommend file be maintained by IAO adding the user to the system.

## EITDR CORE/REGISTRATION QUESTIONS

1. What organization controls the direction for the system?

---

2. What organization(s) contribute funding for the system?

---

3. Who is your AMC A-Staff proponent? (Which directorate?)

---

4. Where does the system operate? Single base or multiple bases (specify locations).

---

5. Name of system: Provide full name of the system

---

6. Acronym of system: Provide abbreviated name of the system

---

7. Description of system: Give a brief paragraph that includes the primary functions that your system performs.

**8. Initiative Type: Select one**

- Organization
- Policy
- Program
- Project
- Special Interest
- System

**9. How is the system owned and operated? Select one**

- GOGO Government (DoD) Owned Government Operated (GOGO)
- GOCO Government (DoD) Owned Contractor Operated (GOCO)
- COCO Contractor Owned Contractor Operated (COCO): includes out-sourced IT services
- COGO Contractor Owned Government (DoD) Operated (COGO)
- NON-DOD: includes Federal, State and local governments, grantees, industry partners, etc.

**10. What type of IT investment is this (System, Initiative, Family of Systems, System of Systems)? Select one**

- System
- Initiative (With no systems)
- Family of Systems (FOS)
- System of Systems (SOS)

**11. Investment State or Life-cycle Phase (Status):** Initial Concept and Planning efforts have no operational or procurement aspects, and should use RDT&E or DWCF Capital funds only. Full Acquisition means procurement is active (planning may also be ongoing) and no capability is yet fielded. Steady State projects should not include any new capability development (fact-of-life upgrades & equipment replacement funding are acceptable). Initiatives that have sub-portions in more than one of the preceding categories are Mixed Life Cycle; most projects using multiple appropriations are likely Mixed Life Cycle investments.

Select one

1. Pre-systems Acquisition: User needs and technology opportunities

\_\_\_\_\_ a. Initial Concept (3600 funds only)

\_\_\_\_\_ b. Initial Concept (3600 funds only)

2. ACQ: Concept Refinement and Technology Development

\_\_\_\_\_ a. Concept exploration

\_\_\_\_\_ b. Component advanced development

3. ACQ: Systems Development and Demonstration

\_\_\_\_\_ a. Concept exploration

\_\_\_\_\_ b. System demonstration

4. ACQ: Operations and Support (Steady State Only -- Sustainment--No development)

\_\_\_\_\_ a. Sustainment

\_\_\_\_\_ b. Disposal (Being Migrated/Decommissioned/Retired)

OR

\_\_\_\_\_ 5. Any two or more checked: Mixed Life Cycle (More than one or overlapping)

**12. Date this capability became/will become operational:**

\_\_\_\_\_

**13. What is your Mission Assurance Category (MAC) Level: I, II, or III?**

Select one

\_\_\_\_\_ MAC I: Vital to operational readiness/mission effectiveness of deployed/contingency forces

\_\_\_\_\_ MAC II: Important to/supports deployed/contingency forces

\_\_\_\_\_ MAC III: System necessary to conduct day-to-day business

**14. Select the Transition Plan State.**

\_\_\_\_\_ Core System: An existing system, a system in development, or a system beginning the acquisition process that is/will become the Department's solution for a given capability(ies), as designated by the Mission Area.

\_\_\_\_\_ Interim System: An existing system or system in development, as designated by the Mission Area that supports the Department for a given capability during a limited period of time. An interim system has the potential to become part of the core solution.

\_\_\_\_\_ Legacy System: An existing system that is designated for closure when the capability is absorbed by an interim or core system. Sunset date may/may not be determined.

**15. What type of National Security System (NSS) is this application/system?**

**Definition of National Security System (NSS): NSS is defined as any telecommunications or information system operated by the Federal Government, or by contractor on behalf of the Government, the function, operation, or use of which:**

- a. involves intelligence activities
- b. involves cryptologic activities relation to national security
- c. involves command and control of military forces
- d. involves equipment that is an integral part of a weapon or weapon system; or
- e. is critical to the direct fulfillment of military or intelligence missions

Select one

\_\_\_\_\_ NSS - Involves Intelligence Activities

\_\_\_\_\_ NSS - Involves Cryptologic Activities Related to National Security

\_\_\_\_\_ NSS - Involves Equipment that is an Integral Part of a Weapon or Weapons System

NSS - Involves Command and Control of Military Forces

NSS - Is Critical to the Direct Fulfillment of Military or Intelligence Missions

NSS - Processes Classified Information

IT (Not NSS)

**16. Primary Mission Area:** Check one in the table below

<input type="checkbox"/>	BMA-FM (Financial Management)
<input type="checkbox"/>	BMA-HRM (Human Resource Management)
<input type="checkbox"/>	BMA-MSSM (Material Supply & Service Management)
<input type="checkbox"/>	BMA-RPILM (Real Property and Installation Lifecycle Management)
<input type="checkbox"/>	BMA-WSLM (Weapon Systems Lifecycle Management)
<input type="checkbox"/>	DIMA-INT (Defense Intelligence)
<input type="checkbox"/>	EIEMA-CES (Core Enterprise Services)
<input type="checkbox"/>	EIEMA-CMPI (Computing Infrastructure)
<input type="checkbox"/>	EIEMA-COM (Communications)
<input type="checkbox"/>	EIEMA-IA (Information Assurance)
<input type="checkbox"/>	WMA-BA (Battlespace Awareness)
<input type="checkbox"/>	WMA-C2 (Command and Control)
<input type="checkbox"/>	WMA-FA (Force Application)
<input type="checkbox"/>	WMA-FL (Focused Logistics)
<input type="checkbox"/>	WMA-FM (Force Management)
<input type="checkbox"/>	WMA-FP (Force Protection)
<input type="checkbox"/>	WMA-JT (Joint Training)
<input type="checkbox"/>	WMA-NC (Net Centric)

**17. Is Interoperability Test Certification required for this system?**

DODI 5000.2 (E.5.1.4.9) requires Joint Interoperability Test Certification for all IT & NSS regardless of Mission Area. All DoD MDAPs, programs on the OSD T&E Oversight list, post acquisition (legacy) systems, and all programs and systems that must interoperate, are subject to interoperability evaluations throughout their life cycles to validate their ability to support mission accomplishment.

Yes

No

**18. Does this system use OR intend to use Internet Protocol (IP) networking for any intra- or inter- systems communications?**

Yes

No

**19. Does your IT investment process/store Privacy Act Information (i.e., social security number, personal data, etc)?** The Privacy Act of 1974 requires DOD (and Components) to publish a system notice in the Federal Register concerning IT systems that contain information about a U.S. citizen or permanent resident alien that is retrieved by the individual's name or some other personal identifier (e.g., SSN, fingerprint).

Personally identifiable information means any information about a U.S. citizen or lawful permanent resident, including but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to identify an individual, either directly or indirectly, such as their name, social security number, date and place of birth, mother's maiden name, gender, race, biometric records, telephone number, email address, etc.

Yes

No

**20. Is there current or planned system modernization?**

10U.S.C. 2222(i)(3) states: The term defense business system modernization means:

(A) The acquisition or development of a new defense business system; or,

(B) Any significant modification or enhancement of an existing defense business system (other than necessary to maintain current services)

Yes

No

**21. Has the investment been certified and accredited?**

Yes

No (if you answered no, please provide a reason as to why your IT investment hasn't been certified and accredited from below)

Pre-Deployment

Embedded IT

Integral to real-time execution

Without Platform Interconnection

Entry does not require C&A

**22. Certification and Accreditation Status:** Select one

System requires C&A but has not gone through the C&A process

System has gone through C&A process and has IATO

Date IATO awarded (if applicable): \_\_\_\_\_

Date IATO expires (if applicable): \_\_\_\_\_

\_\_\_\_\_ System has gone through C&A process and has Full ATO

Date ATO awarded (if applicable): \_\_\_\_\_

Date ATO expires (if applicable): \_\_\_\_\_

**23. Do you have security controls in place?**

\_\_\_\_\_ Yes

\_\_\_\_\_ No

**24. When did you last complete Security Control Testing (i.e. management controls, operational controls and technical controls)?**

Provide a date \_\_\_\_\_

**25. Do you have a Contingency Plan?**

\_\_\_\_\_ Yes

\_\_\_\_\_ No

**26. Have you tested your Contingency Plan?**

\_\_\_\_\_ Yes

\_\_\_\_\_ No

**27. When was the last time your system's Contingency Plan/COOP was exercised?**

Provide a date: \_\_\_\_\_

**28. What was the date of the annual security review?**

Provide a date: \_\_\_\_\_

**29. Does this system require a Plan of Action & Milestones (POA&M)?**

Yes

No

**30. Have you completed a POA&M?**

Yes

No

**31. What date did you submit your POA&M to the Component CIO for consideration?**

Provide a date: \_\_\_\_\_

**Return to AMC/A6-CIO. Direct questions/comments to Ms. Anna Glose or Cyndi Marler, DSN 779-6204/6734.**