DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)

1. CLEARANCE AND SAFEGUARDING

a. FACILITY CLEARANCE REQUIRED: TOP SECRET

b. LEVEL OF SAFEGUARDING REQUIRED: None

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable)*			**3. THIS SPECIFICATION IS:** *(X and complete as applicable)*		
	a. PRIME CONTRACT NUMBER			a. ORIGINAL *(Complete date in all cases)*	DATE *(YYYYMMDD)* 2016XXXXX
	b. SUBCONTRACT NUMBER			b. REVISED *(Supersedes all previous specs)* REVISION NO.	DATE *(YYYYMMDD)*
X	c. SOLICITATION OR OTHER NUMBER XXXXXXXXXXXX	DUE DATE *(YYYYMMDD)* XXXXXXXX		c. FINAL *(Complete Item 5 in all cases)*	DATE *(YYYYMMDD)*

4. IS THIS A FOLLOW-ON CONTRACT? [ ] YES [X] NO. If Yes, complete the following:

Classified material received or generated under _____ *(Preceding Contract Number)* is transferred to this follow-on contract.

5. IS THIS A FINAL DD FORM 254? [ ] YES [X] NO. If Yes, complete the following:

In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____

6. CONTRACTOR *(Include Commercial and Government Entity (CAGE) Code)*

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
TBD		TBD

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

8. ACTUAL PERFORMANCE

a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
377 MSG/CE 2050 Wyoming Blvd SE Kirtland AFB, 87117		377 ABW/IP 4500 Biggs Avenue, SE Kirtland AFB, NM 87117-5776

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

Contracted Base Maintenance Services for the function of Administration Management & Customer Support; Information Management; Engineering Services (Planning & Programming, Design and Construction Management); Real Property Management; Asset Management; Operations Management; Logistics Support (Material Control); Facility & Infrastructure Maintenance & Support; Grounds Maintenance; and Emergency Management & Response for the 377th Civil Engineer Division, Kirtland AFB, NM.

10. CONTRACTOR WILL REQUIRE ACCESS TO:	YES	NO	**11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:**	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	X		a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		X
b. RESTRICTED DATA	X		b. RECEIVE CLASSIFIED DOCUMENTS ONLY	X	
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		X	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		X
d. FORMERLY RESTRICTED DATA	X		d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		X
e. INTELLIGENCE INFORMATION			e. PERFORM SERVICES ONLY		X
(1) Sensitive Compartmented Information (SCI)		X	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		X
(2) Non-SCI		X	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		X
f. SPECIAL ACCESS INFORMATION		X	h. REQUIRE A COMSEC ACCOUNT	X	
g. NATO INFORMATION		X	i. HAVE TEMPEST REQUIREMENTS		X
h. FOREIGN GOVERNMENT INFORMATION		X	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	X	
i. LIMITED DISSEMINATION INFORMATION		X	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		X
j. FOR OFFICIAL USE ONLY INFORMATION	X		l. OTHER *(Specify)* Government Notifications; Security Education and Training; Foreign Disclosure; Dissemination of Export Controlled Technology Data	X	
k. OTHER *(Specify)* SIPRNet; IT/AIS/IS/LAN	X				

12. PUBLIC RELEASE. Any information *(classified or unclassified)* pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release [ ] Direct [X] Through *(Specify)*

All requests for release of information must have the approval of the Program Manager and the 377 ABW/PA Public Affairs Office, Kirtland AFB, NM 87117. Requests should be submitted 60 days prior to expected date of release.
DoD information requested by the media or members of the public or proposed for release to the public by DoD civilians, military personnel, or contractors shall be processed in accordance with DoD Manual 5200.01, *DoD Information Security Program*, DoD Directive 5230.09, *Clearance of DoD Information for Public Release*, DoD Instruction 5230.29, *Security Policy Review of DoD Information for Public Release*, AFMAN 33-302, *Freedom of Information Act Program*, and AFI 35-102, *Security and Policy Review Process*, as applicable.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. *(Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)*

Contractor will be considered an Integrated Visitor Group.

The National Industrial Security Operating Manual (NISPOM) applies, as does applicable DoD and AF guidance associated with Integrated Visitor Group operations conducted on installations, including but not limited to DoD Manual (DoDM) 5200.01, *DoD Information Security Program, Volume 1, Volume 2, Volume 3, and Volume 4* and AFI16-1404 *Air Force Information Security Program* and AFI16-1406 *Air Force Information Security Program* and related Supplements thereto (contractor will notify government Program Manager and/or Contract Officer if guidance clarification is required).

If warranted, Contractor will follow CG-W-5, Joint DOE/DoD Nuclear Weapon Classification Policy and other classification guidance as required and provided to support related mission work. Collateral documents classification marking will be in accordance with E.O. 13526, and DoDM5200.01, *Volume 2, Marking of Classified Information*, 24 Feb 2012, and supplements thereto.

See **DD FORM 254 Security Guidance Continuation Pages** for additional guidance, Addendum/s, and Attachment/s.

THIS DD FORM 254 HAS BEEN REVIEWED AND COORDINATED BY (Digital or Print Name, Org and Sign):

_____
377 ABW/IP

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. [X] Yes [ ] No
(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)
See Performance Work Statement. See DD FORM 254 Blocks 13-15 Security Guidance Continuation Pages. A Visitor Group Security Agreement (VGSA) applies and is required.

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. [X] Yes [ ] No
(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)
Installation commander has elected to retain security cognizance, CSO is relieved of responsibility to inspect. 377 ABW/IP will conduct required inspections IAW DD FORM 254, applicable DoD and AFI guidance, and applicable Visitor Group Security Agreement (VGSA). Other functional experts such as COMSEC, OPSEC, IA/COMPUSEC, etc., may be included when warranted. See Blocks 13-15 Security Guidance Continuation Pages.

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE *(Include Area Code)*
	Contracting Officer	

d. ADDRESS *(Include Zip Code)*	**17. REQUIRED DISTRIBUTION**	
377 MSG/Contracting Division (PZIC) 8500 Gibson Blvd SE, Bldg 20202 Kirtland AFB, NM 87117	X	a. CONTRACTOR
		b. SUBCONTRACTOR
	X	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
e. SIGNATURE		d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
	X	e. ADMINISTRATIVE CONTRACTING OFFICER
	X	f. OTHERS AS NECESSARY 377 ABW/IP, SSA, SSO

DD FORM 254 Security Guidance Continuation Pages

Ref 10a. Communications Security (COMSEC) Information. Contractor will comply with relevant NISPOM provisions in regards to all Communications Security (COMSEC) information and/or Cryptologic (CRYPTO) items. The Contractor will access, handle, and protect COMSEC and/or CRYPTO per direction of government representatives IAW AFMAN33-283 and other guidance/directives as deemed necessary by location/installation COMSEC Manager. Access to COMSEC material by personnel is restricted to U.S. citizens holding final U.S. Government clearances. Such information is not releasable to personnel holding only reciprocal foreign clearances. The Contractor will seek clarification from the government Contracting Officer, Program Manager or 377 MSG/SCXS for any area dealing with COMSEC and/or CRYPTO they are unsure of in regards to procedures, access, handling, safeguarding, etc. The Contractor will make immediate notification to the responsible government security manager and/or 377 MSG/SCXS, of any situation potentially putting at risk any COMSEC or CRYPTO information, material, items, etc.; and if necessary, take immediate safeguarding measures deemed appropriate and reasonable until properly relieved by the government Security Manager, and/or location/installation COMSEC Manager.

Ref 10b. Restricted Data. The Administration Management & Customer Service; Engineering Services (Planning & Programming, Design, Construction Management); Operations Management; and Emergency Management & Response staffs are permitted access to the RESTRICTED DATA (RD) in performance of this contract when directed and approved by the Government; and only at the performance location specified by the organization in 8a, unless specifically authorized and documented otherwise by the government Contracting Officer; and only when all related access requirements stated below have been met. Access to the RD requires a final U.S. Government clearance at or above the appropriate level commensurate with the information concerned. Contractors granted access to RD information will be based on verification of final security eligibility, need-to-know, and only after the individual receives an RD indoctrination briefing. RD is not a dissemination control marking, but instead a unique category of classified information defined by section 2014 of title 42, U.S.C. (also known and hereafter referred to as "The Atomic Energy Act of 1954, as amended." Guidance on policies and procedures governing access to and dissemination of RD, including CNWDI and Sigma categories, which are subsets of RD is provided by DoDI 5210.02. The contractor shall comply with applicable RD provisions in DoDM 5200.01, DoDI 5210.02, and AFI16-1404; and notify the government Program Manager and/or Contracting Officer of any provisions or requirements therein which they are unable to meet or require clarification. Contractor personnel with access to RD must be trained on the procedures for derivative classification, marking, recognizing, and handling RD information and documents. Requests for access to RD in the possession of the DOE or other Federal agencies designated by the DOE, other than DoD will only be made through the appropriate government responsible program management office and utilize DOE Form 5631.20, "Request for Visit or Access Approval." Dissemination of RD information will be made only after the holder of the information has verified: (a) The identification of the prospective recipient, (b) The validity of the prospective recipient's clearance, (c) The need to know of the prospective recipient in connection with official duties. RD is never automatically declassified and such information must not include declassification instructions; never annotate a declassification instruction on documents containing solely RD/FRD. If a RD document also contains classified national security information annotate the "Declassify On:" line with "Not Applicable to RD/FRD portions." Mark RD in accordance with DoDM 5200.01, Volume 2, Enclosure 4. Make every attempt to not comingle RD/FRD/CNWDI with non-RD/FRD/CNWDI classified national security information; notify the government Program Manager if this must be done. The contractor shall maintain a record of individuals with access to RD (and CNWDI if applicable) and associated indoctrination and recurring training details until directed otherwise.

Ref 10d. Formerly Restricted Data. The Administration Management & Customer Service; Engineering Services (Planning & Programming, Design, Construction Management); Operations Management; and Emergency Management & Response staffs are permitted access to Formerly Restricted Data (FRD) in performance of this contract when directed and approved by the Government; and only at the performance location/s specified by the organization in 8a, unless specifically authorized and documented otherwise by the government Contracting Officer; and only when all related access requirements stated below have been met. FRD is not a dissemination control marking, but instead a unique category of classified information defined by section 2014 of title 42, U.S.C. (also known and hereafter referred to as "The Atomic Energy Act of 1954, as amended." Guidance on policies and procedures governing access to and dissemination of FRD is provided by DoDI 5210.02. The contractor shall comply with DoDI 5210.02 and notify the government Program Manager of any provisions or requirements therein they are unable to meet. To have access to FRD an individual must have a valid security clearance at or above the level commensurate with the information concerned, and a need-to-know. There is no special

indoctrination required to have access to FRD. Contractor personnel with access to FRD must be trained on the procedures for derivative classification, marking, recognizing, and handling FRD information and documents. Mark FRD in accordance with DoDM 5200.01, Volume 2, Enclosure 4. Never annotate a declassification instruction on documents containing solely RD/FRD. Make every attempt to not comingle RD/FRD/CNWDI with non-RD/FRD/CNWDI classified national security information; notify the government Program Manager if this must be done.

Ref 10j. For Official Use Only Information. Controlled Unclassified Information (CUI) is the term which collectively refers to certain types of unclassified information which also requires application of access and distribution controls and protective measures for a variety of reasons. Attachment #1, FOR OFFICIAL USE ONLY (FOUO) ADDENDUM, DoD CONTROLLED UNCLASSIFIED INFORMATION ADDENDUM and REPORT OF LOSS OF PERSONAL IDENTIFIABLE INFORMATION ADDENDUM includes requirements for handling of certain types of information; DoDM 5200.01-V4 also applies.

Ref 10k. SIPRNet. Secret Internet Protocol Network (SIPRNet) access is required by the Administration Management & Customer Service; Information Management; Engineering Services (Planning & Programming, Design, Construction Management); Operations Management; Facility & Infrastructure Maintenance & Support; and Emergency Management & Response staffs when directed and approved by the Government. The contractor shall not access, download or further disseminate any special access data (i.e., intelligence, NATO, COMSEC, etc.) outside the execution of the defined contract requirements and without the guidance and written permission of the government Contracting Officer.

Ref 10k. IT/AIS/IS/LAN. Information Technology (IT)/Automated Information System/s (AIS)/Information Systems (IS)/Local Area Network (LAN): The contractor will require access to the government IT/AIS/IS/LAN to perform their contractual duties. Contractors requiring access to government IT/AIS/IS/LAN must meet authorized user access control, training, reporting and other requirements specified by the host installation and as contained in AFMAN33-282, which includes being determined to be trustworthy by a designated government official prior to LAN access being granted. At no time will individual personally owned computer systems be used to support government operations without prior DAA C&A approval. At no time will foreign nationals or foreign government personnel be granted access to any information systems with official government information associated with the contract (either processing or with data at rest) without specific prior approval from GCA and DAA C&A. Ensure all users are warned and provided with appropriate privacy and security notices that the systems they are entering are DoD systems, and thus subject to monitoring, recording and auditing by authorized personnel. In addition, in accordance with HSPD-12, any new applicant for the Common Access Card (CAC) or DOE equivalent, will require an appropriate background investigation prior to issuance of the CAC. Contractor shall report as soon as possible upon learning of cyber intrusions and other compromises of Defense Program Information (DPI) to their supporting counterintelligence office, which will inform the DoD-DIB Common Information Sharing Environment (DCISE). The Contractor will also notify the government Security Manager of any incidents. Loss of CUI will be promptly reported to the Government Security Manager.

Ref 11b Receive Classified Documents Only. Top Secret access limited to Administration Management & Customer Service; and Engineering Services (Planning & Programming, Design, Construction Management) staff personnel as specifically designated/authorized by the Government (currently projected as four individuals). Secret access limited to Information Management; Operations Management; Facility & Infrastructure Maintenance & Support; and Emergency Management & Response staff when directed and approved by the Government. Classified access is not authorized for Real Property Management; Asset Management; Logistics Support (Material Control); and Grounds Maintenance staffs.

Ref 11h. Require a COMSEC Account. Contractor will require access to Communications Security (COMSEC) information and/or Cryptologic items (CYRPTO) only at the on-base location and/or locations under cognizance and/or support of the organization listed in 8a. Contractor will only have access to COMSEC non-accountable and accountable material through the government representative's sub-account. Access will be controlled by the sponsoring agency.

Ref 11j. OPSEC requirements. The contractor will comply with installation OPSEC programs. Contractor personnel will know who their organization's OPSEC coordinator is and contact them for questions, concerns, or recommendations for OPSEC or Signature Management (SM) related topics. AFI10-701 OPSEC requirements apply to include being familiar with the organization's critical information and protecting critical and/or sensitive information from disclosure. Contractor personnel will NOT publicly post or publish work-related information that potentially contains critical or sensitive information without explicit approval of their immediate supervisor, security office and/or OPSEC PM/SM/OPSEC

coordinator, this includes NOT publicly disseminating, or publishing photographs displaying critical and/or sensitive information, nor publicly referencing, disseminating, or publishing critical and/or sensitive information already compromised. When directed or as part of established Standard Operating Procedures, contractor personnel will destroy (burn, shred, etc.) critical and/or sensitive unclassified information no longer needed to prevent the inadvertent disclosure and/or reconstruction of this material and implement additional protection measures as ordered by the commander, director, or an individual in an equivalent position. Contractor personnel will report attempts by unauthorized personnel to solicit critical and/or sensitive information and treat such attempts as human intelligence (HUMINT) gathering and consider it a HUMINT incident. All contractor personnel who have been involved in or have knowledge of a possible HUMINT incident will report all facts immediately to the nearest supporting AFOSI office.

Ref 11l. Government Notifications. The Contractor will notify the government when so directed and/or specified by provisions in this DD FORM 254, related contract and/or related clauses, attachments, addendums, etc. The Contractor will immediately notify the government Contracting Officer of any changes relating to foreign owned, controlled, or influence (FOCI) type concerns, events and/or changes which may affect the Facility Security Clearance (FCL).

Ref 11l. Security Education and Training. Contractor personnel will participate in and receive security education and training at direction of the government Security Manager to include initial, recurring and annual venues, if warranted. Training may include what defines classified information and CUI; proper protection of classified and CUI; actions to take if classified information or CUI is found unsecured, a vulnerability is noted, or a person seeks unauthorized access; a basic understanding of security policies and principles; requirements for public release of DoD/DOE information; personnel responsibilities and the sanctions that can be applied; local threat and techniques foreign intelligence activities use; and other relevant subjects/topics. Training and use of Security Classification Guide/s (SCG/s) will also be done. Contractor personnel not completing required training may be limited or prohibited from doing government work if deemed necessary by the government Program Manager. Related training records should be maintained on file for review by the CSO.

Ref 11l. Foreign Disclosure. Foreign Disclosure of DoD information is not authorized in performance of this contract.

Ref 111. Dissemination of Export Controlled Technology Data. Export of Controlled Technology is not authorized in performance of this contract.

Attachment# 1 to the DD Form 254.
DoD CONTROLLED UNCLASSIFIED INFORMATION ADDENDUM,
FOR OFFICIAL USE ONLY (FOUO) ADDENDUM,
and
REPORT OF LOSS OF PERSONAL IDENTIFIABLE INFORMATION ADDENDUM
CONTINUATION OF DD FORM 254
CONTRACT: XXXXXXXX

DoD Controlled Unclassified Information Addendum:
Ref DD Form 254 block/item 10j. In addition to classified information, certain types of unclassified information also require application of access and distribution controls and protective measures for a variety of reasons. Such information is referred to collectively as Controlled Unclassified Information (CUI). DoD CUI includes For Official Use Only (FOUO), Law Enforcement Sensitive (LES), DoD Unclassified Controlled Nuclear Information (DoD UCNI), and LIMITED DISTRIBUTION, as well as some of those developed by other Executive Branch agencies. Contractors shall comply with related CUI applicable provisions identified in DoDM 5200.01, V-4, dated February 24, 2012.

ALL DoD unclassified information MUST BE REVIEWED AND APPROVED FOR RELEASE through standard DoD Component processes before it is provided to the public. The contractor will notify the Government Contracting Officer of unauthorized disclosures of DoD CUI.
The originator of a document is responsible for determining at origination whether the information may qualify for CUI status, and if so, for applying the appropriate CUI markings.

For Official Use Only (FOUO):
FOUO is a dissemination control applied by the Department of Defense to unclassified information when disclosure to the public of that particular record, or portion thereof, would reasonably be expected to cause a foreseeable harm to an interest protected by one or more of FOIA Exemptions 2 through 9. The document's originator will determine at origination whether the information may qualify for FOUO status and to ensure markings are applied as required.
Contractors will comply with DoDM 5200.01, V-4, dated February 24, 2012. In regards to DoD CUI and related FOUO. The following are select areas of emphasis:

1. ACCESS/DESIGNATION: Access to FOUO material shall be limited to those employees needing the material to do their jobs. No person may have access to information designated as FOUO unless that person has been determined to have a valid need for such access in connection with the accomplishment of a lawful and authorized Government purpose. FOUO is not a classification. When a classified document or portion thereof is declassified, FOUO markings may be applied, if applicable, to protect the information. Marking information FOUO does not automatically qualify it for exemption from public release pursuant to the FOIA. If a request for a record is received, the information shall be reviewed to determine if it truly qualifies for exemption.

2. MARKING: Mark FOUO documents in accordance with DoDM 5200.01, V-4, ENCLOSURE 3, dated February 24, 2012, unless directed by the AF Activity to use approved variations. For example, for any e-mail containing FOUO, ensure the subject line alerts a reader the information includes FOUO (Subject Line Example: (FOUO) SUBJECT XYZ). Also, include the following warning Statement at the top of each email containing FOUO:
This e-mail contains FOR OFFICIAL USE ONLY (FOUO) information which must be protected under the Freedom of Information Act (5 U.S.C 552) and/or the Privacy Act of 1974 (5 U.S.C. 552a). Unauthorized disclosure or misuse of this PERSONAL INFORMATION may result in disciplinary action, criminal and/or civil penalties. Further distribution is prohibited without the approval of the author of this message unless the recipient has a need to know in the performance of official duties. If you have received this message in error, please notify the sender and delete all copies of this message.

3. STORAGE: During working hours, reasonable steps shall be taken to minimize the risk of access by unauthorized personnel (e.g., not reading, discussing, or leaving FOUO information unattended where unauthorized personnel are

present). After working hours, FOUO information may be stored in unlocked containers, desks, or cabinets if Government or Government-contract building security is provided. If such building security is not provided or is deemed inadequate, the information shall be stored in locked desks, file cabinets, bookcases, locked rooms, etc. Expenditure of funds for security container or close areas solely for the protection of FOUO material is prohibited unless specifically authorized by the Government Contracting Officer.

4. TRANSMISSION: FOUO information and material may be transmitted via first class mail, parcel post, or, for bulk shipments, via fourth class mail. Whenever practical, electronic transmission of FOUO information (e.g., data, website, or e-mail) shall be by approved secure communications systems or systems utilizing other protective measures such as Public Key Infrastructure (PKI) or transport layer security (e.g., https). Use of wireless telephones should be avoided when other options are available. Transmission of FOUO by facsimile machine (fax) is permitted; the sender is responsible for determining that appropriate protection will be available at the receiving location prior to transmission (e.g., machine attended by a person authorized to receive FOUO; fax located in a controlled government environment).

5. RELEASE: FOUO material shall not be released outside the contractor's facility except to representatives of the DOD.

6. DESTRUCTION: When no longer needed, FOUO material shall be disposed of by a method that precludes its disclosure to unauthorized individuals.

Report of Loss of Personal Identifiable Information:
Reporting of incidents is required when there is a loss, theft or compromise of PII (i.e. breach). All breaches shall be reported to the government Program Manager and the 377th Air Base Wing (ABW) Privacy Act Officer at (505) 846-7717 immediately. Breaches subject to reporting and notification include electronic systems and paper documents.

Contractors shall:

- Take such actions, as considered appropriate, to ensure that any government personal information contained in a system of records, of which they have access to and are using to conduct official business, shall be protected so that the security and confidentiality of the information shall be preserved.

- Not disclose any government personal information contained in any system of records, except as authorized by applicable laws or regulations. Contractors willfully making such disclosure when knowing that disclosure is prohibited are subject to possible criminal penalties and/or administrative sanctions.

- Report any unauthorized disclosures of government personal information from a system of records or the maintenance of any system of records that are not authorized to the 377th ABW Privacy Act Officer.

- Initial written reports shall be made as expeditiously as possible in all cases within 72 hours of discovery. Additional information may be required after submission and review of the initial report, guidance will be provided at that time. Mark any reports For Official Use Only, identifying exemptions 6 and 7 apply. Initial report content shall include the following information:

- Identify the organization involved.

- Specify the date of the breach and the number of individuals impacted, to include whether they are DoD civilian, military or contractor personnel; DoD civilian or military retirees; family members; other Federal personnel or members of the public, etc.

- Describe the facts and circumstances surrounding the loss, theft, or compromise.

- Describe actions taken in response to the breach, to include whether the incident was investigated and by whom; the preliminary results of the inquiry if then known; actions taken to mitigate any harm that could result from the breach; whether the affected individuals are being notifies, and if this will not be accomplished within 10 working days; what remedial actions have been, or will be, taken to prevent a similar such incident in the future, e.g., refresher training conducted, new or revised guidance issued; and any other information considered pertinent as to actions to be taken to ensure that information is properly safeguarded.