BY THE ORDER OF THE COMMANDER
NORTH AMERICAN AEROSPACE
DEFENSE COMMAND (NORAD) AND
UNITED STATES NORTHERN
COMMAND (USNORTHCOM)

NORAD AND USNORTHCOM
INSTRUCTION 33-194 VOLUME 2

19 SEPTEMBER 2013

Communication and Information

HEADQUARTERS NORAD AND USNORTHCOM INFORMATION GOVERNANCE VOLUME 2 - RECORDS MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: NORAD and USNORTHCOM publications and forms are available on the NORAD and USNORTHCOM portal page for downloading. https://portal.noradnorthcom.mil/library/Pubs/SitePages/Home.aspx.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: N-NC/CSKM Certified by: N-NC/CSD (Colonel Ronald L. Banks)

Supersedes NNCHOI90-123, 1 Apr 05 Pages: 27

This instruction implements the Joint Staff records management program, CJCSM 5760.01A, *Joint Staff and Combatant Command Records Management Manual, Volume I (Procedures)* and *Volume II (Disposition Schedule)* within the North American Aerospace Defense Command (NORAD) and the United States Northern Command (USNORTHCOM). This instruction applies to all NORAD and USNORTHCOM organizations, subordinate unified Commands, joint task forces and all other subordinate functional components or operational forces that remain directly responsive to the Commander (CDR), NORAD and USNORTHCOM. It does not apply to Air Force Reserve Command or National Guard units. This instruction may not be supplemented. Send recommendations to change, add, or delete information in this instruction to HQ NORAD and USNORTHCOM, ATTN: N-NC/CSKM, 250 Vandenberg Street, Suite B016, Peterson AFB, CO 80914-3020 using AF Form 847, *Recommendation for Change of Publication*. Maintain and dispose of records created as a result of prescribed processes in accordance with the Joint Staff Disposition Schedule CJCSM 5760.01A, Vols. I & II. See **Attachment 1** for a list of references and supporting information.

1. Policy. It is the policy of the CDR NORAD and USNORTHCOM that all personnel will comply with the following:

1.1. Create, maintain, preserve, and dispose of records that document the roles and activities of the Commands in the conduct of assigned missions as directed by CJCSM 5760.01A, Vols. I & II.

1.2. Provide for a continuous set of records reflecting the organization, functions, policies, procedures, operations and other actions of the Command that have historical, legal, research, or public interest value.

1.3. Identify and maintain vital business information and records.

1.4. Retain record copies of documents, in all media and formats, regardless of format, environment or type of media, until such time as they are eligible for disposition according to CJCSM 5760.01A, Vol. II.

1.5. Release information to agencies (other Department of Defense (DOD) Components, Executive branch agencies, contractors, auditors, and Congress) not on original distribution if the agencies have a validated need to know, hold the appropriate level of security clearance, and if the release is within any limitations specified on the document.

1.6. Understand the official definition of a record to be "... all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the U.S. Government under Federal law or in connection with the transaction of a public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of the data in them." (44 U.S.C. § 3301) A record "bucket" is a type of flexible schedule in which disposition instructions are applied against a body of records that are grouped.

1.7. Understand that failure to observe the prohibitions and mandatory provisions of this instruction by military personnel is a violation of Article 92, *Failure to Obey Order or Regulation*, Uniform Code of Military Justice. Similarly, failure to observe the prohibitions and mandatory provisions of this instruction by civilian personnel may result in administrative disciplinary action and applicable civil and criminal sanctions for violation of Federal Law, punishable by fines, imprisonment or both. (18 U.S.C. § 2071) The contracting office is responsible for including record management language in contracts.

1.8. Applicability. This instruction applies to all Headquarters NORAD and USNORTHCOM directorates, special staff, subordinate and direct reporting units, and activities that create NORAD and/or USNORTHCOM records.

1.8.1. This instruction does not apply to Service components and their single Service Commands creating service-specific records, who will comply with their respective Service records management directives.

1.8.2. Records produced by or received from external organizational equities (ex: Defense Intelligence Agency, National Reconnaissance Office, etc.) will follow their respective records management directives.

2. Responsibilities and Duties.

2.1. Chief of Staff. Oversee the NORAD and USNORTHCOM Records Management Program.

2.2. Corporate or "Top 3 (U.S.)" Records. All records from the offices of the Commander, USNORTHCOM Deputy Commander and Chief of Staff ("Top 3 (U.S.)") are considered permanent records and must be maintained in accordance with Record Bucket 0000-04-CC of CJCSM 5760.01A, Vol. II. The Secretary to the Joint Staff office has been designated by the Commander, as responsible for the physical custody, maintenance, and disposition of corporate records.

2.2.1. At the discretion of the Commander, he/she may select additional positions or offices of such importance that the records created within them are also considered permanent. Examples include, but are not limited to, additional Deputy positions or the Senior Enlisted Advisor. These positions, collectively, are considered "**Top 3 (U.S.)**" and records created within their respective offices will be maintained in accordance with (IAW) Record Bucket 0000-04-CC of CJCSM 5760.01A, Vol. II

2.3. Commands Records Manager (CRM). Develops, implements, supervises, and manages the Records Management (RM) program, to include developing processes and ensuring procedures are carried out according to Federal Statutes and regulations. The CRM:

2.3.1. Ensures the Commands have an up-to-date records management directive.

2.3.2. Serves as the primary official who coordinates RM matters with National Archives and Records Administration (NARA), Chairman of the Joint Chiefs of Staff (CJCS) Information Management Division and other oversight agencies.

2.3.3. Coordinates matters relating to RM with the Commands' Freedom of Information Act (FOIA) and Privacy Act office, Chief Information Officer, System Administrators, Program Managers, Inspector General, Staff Judge Advocate, Public Affairs Office, and

Historian Office (HO), as well as the Multimedia office or other officials responsible for special media.

2.3.4. Ensures that record-keeping requirements are established, implemented and periodically updated for all offices of record, including direct reporting and subordinate units, and for all media types.

2.3.5. Ensures all directorates and special staff offices, including those at direct reporting and subordinate units, appoint, in writing, a primary and alternate Records Officer (RO) at the directorate level, or equivalent.

2.3.6. Ensures all directorates and special staff offices, including those at direct reporting and subordinate units, appoint, in writing, Files Custodians (FC) at the division and branch levels, or equivalent, if applicable, to ensure each office of record has at least one appointee.

2.3.7. Trains, directs, and provides guidance to all ROs.

2.3.8. Directs ROs to develop and implement File Plans in accordance with CJCSM 5760.01A, Vol. II.

2.3.9. Ensures ROs provide necessary training and guidance to FCs in order to fully implement the RM program.

2.3.10. Serves as the approval authority for all File Plans, which shall be created by using the Commands' File Plan Database. This database takes the place of the Joint Staff Form 31, List of Selected Files Numbers.

2.3.11. Provides guidance for records collections and retention in mobilization planning and crisis action procedures, to include Command operations center records.

2.3.12. Provides guidance to ensure records management annexes are included in appropriate operations plans, operations orders, and concept plans.

2.3.13. Provides guidance on record keeping requirements for electronic information systems (EIS) during development/design, prior to implementation.

2.3.14. Completes and submits annual and special records management reports, as required, to CJCS and the NARA.

2.3.15. Works with each RO to make sure that all offices of records are represented on the File Plan.

2.3.16. Works with ROs to ensure the transfer of eligible records to the Commands' staging facility or a Federal Records Center (FRC); the prompt disposal of temporary records when their retention period expires; and the timely transfer of permanent records to NARA.

2.3.17. Prior to disposing any temporary records eligible for destruction, coordinates with the Command Historian (HO) to identify historically important records for inclusion in the Command's archive.

2.4. Directorate and Special Staff Offices. Directors and Special Staff office chiefs, to include those at direct reporting and subordinate units, are responsible for full implementation and supervision of the RM program within their organization. The Director or Special Staff Office Chief:

2.4.1. Appoints, in writing, a primary and alternate RO to manage, under the direction of the CRM, the RM program within their organization. It is recommended that the RO be an O-3 or higher, or GS equivalent, with at least twelve (12) months remaining on Command assignment, and with clearance to view/access content at the highest level created within the organization. No contractors shall be appointed as a RO. Directorates will provide an appointment letter (see **Attachment 2** for example) to the CRM within three days of appointment. Do not include Privacy Act information, such as social security number, on the appointment letter.

2.4.2. Appoints, in writing, a FC at each division and/or branch level, to ensure each office of record has at least one FC appointed. The appointment of FCs at branch level shall not be based on the size of the branch, but on the nature of the business of the branch and the extent to which the appointed FC can properly perform his/her RM duties. Each FC must have clearance to view/access content at the highest level created within the office of record.

2.4.3. Ensures the prevention of mutilation or unauthorized disposition of records in all media. Unauthorized disposition is the removal from NORAD and USNORTHCOM custody, to include all direct reporting and subordinate units, or destruction of records without regard to the provisions of approved disposition schedules according to CJCSM 5760.01A, Vol. II. Examples of unauthorized disposition might include, but are not limited to:

2.4.3.1. Saving a record due for destruction under a new file name and reapplying a new disposition to the same record content

2.4.3.2. Saving a record due for destruction as a reference copy

2.4.3.3. Printing and/or saving a record due for destruction in a personal file or directory.

2.4.4. Ensures ROs and FCs are scheduled for initial training within 30 days of appointment and attend refresher training as needed, but at least annually.

2.4.5. Ensures records are created, maintained, and preserved to document the organization, functions, policies, decisions, procedures, and essential operational, logistical, and support transactions of the organization. Supporting materials should be incorporated into the record copy file of the action.

2.4.6. Ensures personnel are aware they must inform their RO, FC and/or the CRM of any actual, impending, or threatened unlawful removal, alteration, or destruction of records, to include electronic records. Notification must include a description of any such records, circumstances in which unauthorized destruction took place, and corrective steps being taken to properly manage records in future.

2.4.7. Ensures personnel safeguard all personal data within records, in accordance with DOD 5400.11-R, ***Privacy Program*** and **5 U.S.C. § 552a, *Privacy Act*** and identify within your File Plans those sub-buckets (record series) that might contain Personally Identifiable Information. Additionally, any Record Buckets identified MUST include access controls/identification of security groups within the approved organization File Plan to restrict access within the Records Repository.

2.4.8. Ensures personnel support the RM program with timely responses to reporting requirements from the CRM.

2.4.9. Appoints, in writing, a Destruction Validation Officer (DVO) to validate records ready for disposition, as presented by the CRM. The DVO should be a senior officer (Division/Deputy Division Chief) having the authority to certify the destruction of government records, with at least twelve (12) months remaining on Command assignment, and with clearance to view/access content at the highest level created within the organization. No contractors shall be appointed as a DVO. No RO or FC shall be appointed as DVO. Directorates and Special Staff offices will provide an appointment letter (see **Attachment 2** for example) of the DVO to the CRM within three days of appointment.

2.4.10. Ensures personnel (to include contractors) transfer records to appropriate repository prior to departing or exiting organization by implementing procedures to prohibit records from being destroyed or lost.

2.4.11. Validates identified vital records and creates a process to ensure access and use during continuity of operations (COOP) or other emergency situations, keeping in mind that network/local area network access may not be available.

2.5. Records Officer (RO), Primary and Alternate. Serves as the point of contact to implement and enforce all aspects of the RM program within the organization, as directed by CRM. The RO:

2.5.1. Attends records management training within thirty (30) days of appointment. Newly appointed ROs will contact the CRM office to schedule training.

2.5.2. Provides training and guidance to all FCs within the organization. Provides an appointment letter, signed by the chief/director of the division or branch and by the new FC acknowledging his/her appointment as a Files Custodian. See **Attachment 2** for example appointment letter.

2.5.3. Assists all FCs in development, submission and implementation of a File Plan by using the Commands' File Plan Database. Reviews, makes necessary changes to and approves File Plans before submission to the CRM for final approval. Ensures electronic records are accounted for and filed in accordance with approved File Plan. RO will submit any updated File Plans to CRM for re-approval within thirty (30) days of update.

2.5.4. Conducts a RM Staff Assistance Visit (SAV) in each office of record at least once annually, or whenever there is a significant change in organization, function, personnel, or as directed by CRM. Each SAV must include a review of the File Plan for updates and changes, which shall be submitted the CRM for approval.

2.5.5. Records the SAV on JS Form 32, Joint Staff/Combatant Command Records Management Inspection List. Follows-up on corrective actions taken for noted discrepancies. Ensures corrective action is completed within thirty (30) days. Sends a copy of the SAV report, including the corrective action, to the CRM.

2.5.6. Ensures electronic records are filed in accordance with the approved File Plan and available to assigned personnel, not mixed with personal papers and non-record materials, and ensures records are not kept in personal drives, personal sites, social media repositories and/or personal e-mail.

2.5.7. Ensures all personnel maintain, service, and manage records of the office according to CJCSM 5760.01A, Vols. I & II, and this instruction. Reminds all personnel not to remove, dispose of or delete records, including electronic records, without proper authorization.

2.6. Files Custodian (FC). Responsible for managing the life cycle of the records of the organization within the FC's area of responsibility, according to CJCSM 5760.01A, Vols. I & II. This includes but is not limited to maintaining, safeguarding, and disposing of records, including electronic records, according to prescribed standards. The FC:

2.6.1. Attends RM training within thirty (30) days of appointment. Newly appointed FCs will contact the organization RO to schedule training.

2.6.2. Develops and implements a File Plan for his/her area of responsibility as directed by CJCSM 5760.01A, Vols. I & II. Ensures that all records for his/her area of responsibility, including electronic records, are listed in the File Plan. Ensures a print out of the File Plan is available to all office personnel and advises the RO of changes as they occur, by submitting an updated File Plan to the RO and CRM. Ensures a print out of the approved File Plan is placed in/on the first file of any file cabinet used for paper records.

2.6.3. Follows the organization's File Plan, including:

2.6.3.1. Systematic file cut-offs (breaks)

2.6.3.2. The retirement of eligible records to a records center

2.6.3.3. The prompt disposal of temporary records when their retention periods expire

2.6.4. Cooperates with the RO and CRM in periodic evaluations of the organization's records.

2.6.5. Ensures electronic records are filed in accordance with the approved File Plan and available to assigned personnel, not mixed with personal papers and non-record materials, and ensures records are not kept in personal drives, personal sites, social media repositories and/or personal e-mail.

2.6.6. Ensures all personnel maintain, service, and manage records of the office according to CJCSM 5760.01A, Vols. I & II and this instruction. Assists RO in reminding all personnel not to remove, dispose or delete records, including electronic records, without proper authorization.

2.6.7. Assists RO in implementing procedures for departing personnel to prohibit them from misidentifying or destroying ineligible records, or removing records from Command custody. *Unauthorized disposition can carry a fine and up to three (3) years in prison. (18 U.S.C. § 2071).*

2.6.8. Ensures each office of record within his/her area of responsibility completes the Records Inventory Worksheet (**Attachment 3**) in order to better identify the types of records each office of record creates in order to ensure that it is captured on the File Plan.

2.7. Destruction Validation Officer (DVO). Responsible for validating records identified as ready for disposition (either destruction or transfer to NARA), were properly metadata tagged or otherwise identified within a records bucket and are, in fact, ready for disposition. The DVO:

2.7.1. Coordinates with his/her ROs and FCs, when required, to ensure that records ready for destruction, presented by the CRM, can, in fact, be destroyed. Validation includes that records were properly tagged or otherwise identified within a records bucket at origination and that the system generated disposition date is correct for that records bucket and cut-off time.

2.7.2. Provides the CRM certification of a record or list of records which are eligible for disposition within thirty (30) calendar days of receiving any disposition report.

2.7.3. May request retention re-assignment of any record; however, the DVO is not authorized to reassign disposition of any record in order to keep them longer than legally prescribed in CJCSM 5760.01A, Vol. II. If any record is found to be incorrectly assigned retention (or metadata tagged) and needs to be re-assigned retention, the DVO shall provide written justification to the CRM within thirty (30) calendar days. If approved by the CRM, the record(s) will be re-assigned by a member of the Command Records Office. Any such justification will include:

2.7.3.1. Concise description of the record series for which the re-assignment is requested

2.7.3.2. Precise list of the records within the record series for which the re-assignment is requested

2.7.3.3. Clear justification for re-assigned retention

2.7.4. May request approval of a temporary extension of a retention period not to exceed one year. The request shall include:

2.7.4.1. Concise description of the record series for which the extension is requested

2.7.4.2. Precise list of the records within the record series for which the re-assignment is requested

2.7.4.3. Estimated period of time that the records will be required, if less than one year

2.7.4.4. Clear justification for extended retention – (operational, audit, legal etc).

2.8. Site Owner/Site Collection Owner (SO/SCO). Until such time as all organization’s File Plans are approved and the Commands technically enforce the Record Bucket as a required field, SO/SCOs must ensure that all Portal libraries are pointed to the correct portion of the Commands’ Record Bucket within the Library Settings (e.g. a library existing on the N-NC/J7 Front Office site is pointed to N-NC/J7 Front Office portion of the Record Bucket) and that the field is marked required. Additionally, assist in adding and configuring any Records Repository search web-parts.

2.9. Operations and Maintenance (O&M) Organization(s). System administrators must notify the CRM, RO and FC whenever system changes may affect electronic records. Backups of the records must be rotated to ensure properly disposed of content no longer resides within a backup copy.

2.10. N-NC/J6. Appoints, in writing, a primary and alternate EIS Manager. The EIS Manager should be an individual involved with architecting or approving any new or enhanced EIS (databases, software applications/programs, electronic logs, etc.), or involved with the service retirement (stand-down) of any EIS, with clearance to view/access content at the highest level created within the organization. No contractors shall be appointed as an EIS Manager. No RO or FC shall be appointed as EIS Manager. N-NC/J6 will provide an appointment letter (see **Attachment 2** for example) to the CRM within three days of appointment. Do not include Privacy Act information, such as social security number, on the appointment letter. The EIS Manager:

2.10.1 . Coordinates new or enhanced EIS with the CRM to ensure any NORAD and USNORTHCOM records created within the new or enhanced EIS are scheduled, captured and/or managed IAW with CJCSM 5760.01A, Vols. I & II and this document.

2.10.2. Assists organizations in completing EIS Questionnaire (see **Attachment 4** for example)

2.10.3. Submits the completed EIS Questionnaire to the CRM prior to implementing any new or enhanced EIS

2.10.4. Assists in the identification of existing EIS that have not been scheduled or were implemented prior to the release of this governance instruction.

2.10.5. Coordinates with the Chief of Staff Knowledge Management Privacy Act office if any EIS contains or is intended to contain Privacy Act information

2.10.6. Coordinates with the CRM prior to any service retirement of an existing EIS to ensure proper, compliant disposition of any records contained within

2.11. End-Users/All users. Responsible for recognizing that the organization's records, including electronic records, are government property and consist of information required by law or used to conduct Command business. The end-user:

2.11.1. Creates and maintains records documenting organization activities and posts/saves them in appropriate Enterprise repositories with applicable metadata.

2.11.2. Cooperates with the CRM, RO and FC to ensure all records, including electronic records, are listed in the approved File Plan.

2.11.3. Does not, when using existing records as templates – including those in any task management system - simply type over existing content, but creates a new record and edits as needed.

2.11.4. Does not mix records with personal papers or non-record materials and ensures records are not kept in personal drives, personal sites, social media repositories and/or personal e-mail.

2.11.5. Cooperates with the CRM, RO and FC in transferring eligible temporary records to a records center and permanent records to NARA.

2.11.6. Cooperates with the CRM, RO, FC and DVO in nominating for/validating deletion of records that have met their legal disposition, however, they do not remove, dispose or delete records, including electronic records, without proper authorization.

3. Joint Staff and Combatant Command Filing System. The RM program provides for the separation of records into distinct categories (Record Buckets), to facilitate referencing and disposition. The filing system is based on functions and not an organizational relationship. The major categories are listed in **Table 1.** below.

Table 1. Major Categories for Joint Staff and Combatant Command Filing System.

Category/Series	Content
0000	Joint Staff (JS) Top 5 and Headquarters (HQ) Combatant Command Records
0100	Organization, Manpower, Committee and Board Records
0200	Personnel and Payroll
0300	Intelligence and Security
0400	Military Justice, Legal, Protocol and Public Affairs
0500	Command and Control (C2), Operations, Planning and Exercises
0600	Logistics, Acquisitions, Supply, Services, Budget and Safety
0700	Communications, Cryptology and Electronics Policies, Procedures and Reports
0800	International
0900	General Administration and Management
1000	Information Technology (IT) Procurement, Planning, Operations and Management
1100	Medical

3.1. Documentation and Filing. The documentation process refers to the creation, assembly, and consolidation of background materials that fully explain or support a specific action in the file. Incomplete documentation can lead to misinterpretation or misunderstanding; therefore, effective documentation practices are essential to ensure that files contain complete accounts of actions taken, commitments made, and the results thereof. These supporting materials should be incorporated into the record copy case file of the action.

3.2. Personal Papers. Personal papers are documentary materials belonging to an individual that are not used to conduct agency business are considered personal papers. These records are related solely to an individual’s own affairs or used exclusively for that individual’s convenience. As such, they must be clearly designated as personal, and kept separate from official records. Classified information must not be included in personal papers. All content, whether personal or official, is subject to FOIA requests and e-Discovery inquiries and must be declared, produced or provided upon request.

3.2.1. Correspondence designated "personal" or "private" but relating to the conduct of public business is an official record subject to maintenance and disposal procedures, regardless of any such designation. Official records are public records and belong to the office, rather than the official or individual.

3.2.2. Official business mentioned in personal papers shall be extracted from the personal papers and made a part of the official record(s).

3.2.3. Questions concerning the distinction between personal and official records should be referred to the office of the Staff Judge Advocate (JA).

3.3. Contingency Records. Joint Task forces, Dual Status Commanders, and Joint Support Force Staff Elements, and any NORAD and USNORTHCOM personnel deployed as a result of crisis or contingency operations must ensure that records requiring collection and preservation are appropriately administered in accordance with CJCSM 5760.01A, Vols. I & II.

3.4. Vital Records and Vital Business Information. Vital records and databases are those documents, references, records, and information systems needed to support Mission Essential Functions (MEF) during a continuity event and include those records and information systems necessary for reconstitution to normal operations after (a) crisis.

3.4.1. Vital records must be accessible by continuity personnel from designated alternate facilities within 12 hours after activation of continuity plans. In some cases, mission requirements will dictate more rapid or even real-time responsiveness.

3.4.2. The two basic categories of vital records and associated requirements for their management are defined as follows:

3.4.2.1. Emergency Operating Records. These include records (to include databases and vital data) essential to the continued functioning or the reconstitution MEFs during and after a continuity event. Examples of these records are operational data, emergency plans and directives, orders of succession, delegations of authority, staffing assignments, and related policy or procedural records. These records provide continuity personnel with the guidance they need to conduct operations during a continuity situation and to resume normal operations at the conclusion of that situation.

3.4.2.2. Rights and Interests Records. These include records (to include databases and vital data) critical to carrying out essential legal and financial functions, and vital to the protection of the legal and financial rights of individuals who are directly affected by NORAD and USNORTHCOM activities. These records include those with such value that their loss would significantly impair the execution of MEFs, to the detriment of the legal or financial rights and entitlements of DOD components and affected individuals. Examples of these records could include copies of contracts to know what can/cannot be legally tasked to contractors, financial responsibilities on which the Commands cannot default, system manuals or documentation, building plans, login/account information or anything needed to accomplish emergency operations.

3.4.3. Vital business information is that which is needed to perform required operations following an emergency and sustain mission operations for as long as thirty (30) days or more.

3.4.4. Records necessary to carry out essential business operations in time of emergency must be maintained in a current status and duplicated or otherwise made available at the COOP location.

3.4.5. Each Directorate and/or Special Staff office must determine what records are considered vital to their organization's mission and identify those records in the File Plan. A member of the leadership of that organization (not the RO or FC) must validate identified vital records. After identification, each Directorate and/or Special Staff office must establish a process to keep those vital records in a current state and determine how to get vital records to any established COOP location. While N-NC/J6 is responsible for maintaining backups and replicating data to the COOP location, consideration must be given for emergencies or disasters in which there is no access to NORAD and USNORTHCOM networks and/or repositories, as well as the handling of classified material during emergency situations and operations. (See **Attachment 5** for a sample of questions to assist in the identification of vital records.)

3.5. Contractor Records. Contractor developed records are subject to NORAD and USNORTHCOM records management requirements. Any contract between NORAD and USNORTHCOM and any contractor must contain specific instructions regarding the safe-guarding, maintenance, and delivery of all data needed for the adequate and proper documentation of the contractor-operated program(s) in accordance with Federal Acquisition Regulation. The contract must specify government ownership of records at the conclusion of the contract.

3.5.1. Research contracts should specify the delivery of background data that have reuse value to the Commands or other government agencies.

3.5.2. Deferred ordering and delivery of data clauses must be included in contracts whenever it is impossible to identify in advance all records and data that may be delivered to the Commands. These clauses enable NORAD and USNORTHCOM officials to acquire additional data that may have reuse value.

3.5.3. Contractors shall treat all deliverables under a contract as the property of the US Government and protect those records according to CJCSM 5760.01A, Vols. I & II and this instruction. Government shall have unlimited rights to use, dispose of, or disclose data contained therein as it determines to be in the public interest and IAW CJCSM 5760.01A, Vols. I & II.

3.5.4. Contractors shall comply with the Federal and NORAD and USNORTHCOM records management policies, including those policies associated with the safeguarding of records by the Privacy Act of 1974. Contractors shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally exempted by the Freedom of Information Act.

3.5.5. The contracting office is responsible for including record management language in all contracts. If any specific records management language is needed based on the nature of a contract, it will be coordinated with the CRM prior to addition into a contract.

3.6. Social Media. NORAD and USNORTHCOM content posted on social media sites (Facebook, Twitter, YouTube, etc.) and within social media repositories are subject to NORAD and USNORTHCOM records management requirements, even though NORAD and USNORTHCOM has no administrative control over any such repository. Offices responsible for monitoring or maintaining content, including public comments and posting responses, will need to develop procedures to identify what information qualifies as a social media record, and capture the content that is not under the control of NORAD and USNORTHCOM, so that all content, both NORAD and USNORTHCOM and that from the public, are saved to the Records Repository, and tagged with the appropriate records management metadata.

3.7. Electronic Mail (e-mail). DOD e-mail systems are for official use only by authorized personnel. The information in these systems is departmental, is only authorized for minimal personal use, as stipulated by JER 5500. In any case, no expectation of privacy or confidentiality applies. Users of DOD e-mail systems will manage any electronic mail message, record of transmission and receipt date, or attachment which meets the definition of a Federal record. Users WILL NOT dispose or cause the disposition of e-mail records without proper authorization of the CRM.

3.7.1. All official e-mail, including attachments, will be treated as electronic records. The originator and action recipient of the e-mail are both responsible for ensuring the preservation and proper disposition of their e-mail comply with CJCSM 5760.01A, Vols. I & II.

3.7.2. Official e-mail of Top 3 (U.S.) will be maintained IAW **paragraph 2.2.** of this instruction via “journaling” or automatic capture at the server by the N-NC/J6 and/or O&M organization and subsequent transfer to the Records Repository.

3.7.3. All personal e-mail which does not meet the definition of a Federal record will be clearly designated as such and either deleted, or maintained separately from any Commands’ records/Records Repository.

4. Records Control. The success of any records system depends upon several basic steps, in accordance with NARA-approved disposition schedules, such as: Identifying and listing records for use; Preparing guides and folders; Creating electronic folders or libraries on information systems; Applying appropriate metadata; Sorting and preparing materials for filing; Locating materials in the files or electronic libraries; Checking materials out to users; Keeping records orderly; Destroying no longer needed reference copies; Transferring inactive hard-copy records to staging facility or permanent records to NARA.

4.1. All records maintained by an office must be identified on the approved File Plan, to include electronic records or EIS and related documentation, action officer files, etc. File plans must identify classified records, vital records, and records containing Privacy Act information. Do not use classified titles on the File Plan.

4.2. File Plan Reviews. ROs/FCs will review the File Plan annually, including a review of electronic files, and submit changes to the CRM for approval.

4.3. Hard Copy Records (Labels, Guide Cards, and Folders). Personnel will follow the examples provided in CJCSM 5760.01A, Vol. I, for all paper records. Labels should include enough information, such as series number and whether or not records are "active" or "inactive," to correctly identify records kept in the drawer. If only one series is filed in a drawer or binder, the label should include cutoff and disposition.

4.4. Sorting and Preparing Materials for Filing. Carefully categorize or metadata tag records by series, in accordance with CJCSM 5760.01A, Vols. I & II, to assure historical, administrative, legal, and research value to NORAD and USNORTHCOM, as well as their relationship to relevant records and their relationship to organization and archival usefulness.

4.4.1. Electronic records, including e-mail, shall be managed and/or tagged with their appropriate records bucket metadata and archived to the Records Repository upon finalization.

4.4.2. Any paper record may be scanned and maintained as an electronic record. Scanning shall only be done in a manner that allows for the content within the scan to be indexed and searchable (using optical character recognition capability vice scanning as an image). This allows for rapid search of documents using metadata or key words. The paper copy may be destroyed after verification that the scanned copy is accurate, readable, retrievable, and the electronic copy is tagged with appropriate records bucket metadata and archived to the electronic records management application (HP TRIM) or Records Repository upon finalization.

4.5. Cut-off and Retention. For paper records, follow specific procedures according to CJCSM 5760.01A, Vol. II. File cut-off is the segregation of active and inactive files and/or the termination of a file after a specified time or event. Periodic file cut-off is essential to control the accumulation of documentation effectively and economically dispose of material in convenient blocks. For electronic files within the Records Repository, cut-off will be monthly for six-month retentions, annually on 31 December for calendar year (CY) retentions and annually on 30 September for fiscal year (FY) retentions. Exception or event-driven retentions will be handled on a case-by-case basis.

4.6. Perpetual Files. Case, action, or project files are kept in active status until the occurrence of a certain event. Review these files at least semi-annually to determine their status. Then, archive, transfer or dispose of them per CJCSM 5760.01A, Vol. II.

4.7. Record Sets of Directives/Publications. Official case files for each organization’s issuances will include the original (or scanned copy of original) signed documents, coordination papers and supporting documents of historical value. All HQ NORAD and USNORTHCOM operating instructions (NNCHOI) record sets, notices, and policy letters are maintained by the Publications and Forms office (N-NC/CST). All other copies are reference copies.

4.8. Disposition. The records disposition standards in CJCSM 5760.01A, Vol. II constitute authority for retention, transfer, temporary or permanent retirement, and/or destruction of record and non-record material, including paper files, files on shared drives or within any electronic repository. Transfer, retire, or destroy/delete eligible records, including electronic records, only in accordance with these disposition instructions. The DVO will certify the list of records eligible for destruction/transfer provided by the CRM prior to the CRM taking action. The CRM will also coordinate with the N-NC/HO to identify historically important records, paper or electronic, for inclusion in the Command’s archive.

4.8.1. Staging. In coordination with the CRM, send applicable paper CY and FY records to the staging area according to the schedule announced each year—generally within sixty (60) days of the cutoff date – to the appropriate staging (storage) facility or records center. Electronic copies may be stored in any electronic format. Electronic records that reside within the Records Repository will be transferred to a staging facility or NARA, by the Command Records Management Office, in coordination with the N-NC/J6 and O&M organization.

4.8.2. Records with a Retention Period of Less than 10 Years. NORAD and USNORTHCOM organizations may keep these paper records in the office of record and, with coordination of the CRM, destroy or delete at the end of the prescribed retention period. Before destruction, the office of record will offer the records to the N-NC/HO. If file volume exceeds storage capacity in the office of record, contact the CRM office to discuss alternative storage facility options. Electronic copies may be stored in authorized electronic repository.

4.8.3. Retention Period of 10 Years or Longer. Paper records should be kept in the office of record for five (5) years, and then sent to the appropriate storage facility or FRC for the remainder of the prescribed retention period. Electronic records may be kept in the Records Repository or pre-accessioned to the FRC or NARA. Permanent records are transferred, legally, to the NARA for retention after twenty-five (25) years. If file volume exceeds storage capacity in the office of record, contact the CRM office to discuss alternative storage facility options. Electronic copies may be stored in authorized electronic repository.

4.8.4. Disposition of Classified Files**.** Observe security requirements when disposing of or shipping classified material.

5. Records Requiring Special Handling or Disposition. FRCs are limited to handling documents up to and including TOP SECRET only. Coordinate with the CRM for the transfer of any NORAD and USNORTHCOM records to ensure they are sent to an appropriately cleared storage facility or records center. Secret Compartmented Information, North American Treaty Organization (NATO), or SIOP records must be retained in the office of record or records holding area until such time as they are downgraded or declassified per DOD 5200.1-R.

5.1. NATO and NORAD-Only Records. Keep NATO and NORAD-only (those without NC affiliation) files separate from non-NATO or NC files. NATO or NORAD-only paper records may be contained within the same approved security container with non-NATO or NC material, under any series number, provided a file divider separates them. NATO or NORAD-only records MAY NOT be kept in the same electronic libraries or folders as non-NATO or NC records. Separate folders, libraries or repositories must be created.

5.2. Transferring Classified Records. Before transferring classified permanent paper records to NARA, the FC/RO and CRM must have command SMEs review all classified records to determine whether or not they can be downgraded or declassified per DOD 5200.01-Vols. 1 & 2. The FC/RO must certify on Standard Form (SF) 135, Records Transmittal and Receipt, the downgrading/declassification review was completed, and indicate appropriate changes, as necessary, on each document.

6. Managing Electronic Records. Official information should reside on shared media and electronic libraries that are accounted for on the File Plan. CJCSM 5760.01A describes essential procedures to manage and protect records, with no distinction of paper or electronic, and to ensure the integrity of all records throughout their life cycle. Records management procedures apply to all EIS, including databases and automated systems.

6.1. New or Enhanced Electronic Information Systems. The EIS Manager notifies and coordinates with the CRM on all proposed, new or enhanced automated or electronic systems where the electronic records are the only or official copy of the records. Data contained in these systems must be retained until the system has been scheduled and disposition authority has been approved by NARA. The EIS Manager, program manager, and office of primary responsibility (OPR) must create and coordinate the records management plan for the system; the plan must identify the frequency for data backup. If Privacy Act information is to be kept within an EIS, coordination with the Commands' Privacy Act Office is also required. If Privacy Act information is going to be kept in any EIS (or other electronic media, such as a spreadsheet), the Commands Privacy Act Office will need to be made aware and a System of Record Number will need to be approved for the system by the DOD Privacy and Civil Liberties Office.

6.2. The RO/FC ensures all electronic records are maintained according to CJCSM 5760.01A by ensuring official electronic records are transferred to a new system during system termination and upgrade. In the event of a loss of records, the RO/FC submits a report per paragraph 8 of this HOI. If records are maintained on a system drive, the System Administrator must notify the FC, RO, and CRM whenever system changes may affect records. Backups of the records must be maintained for the longest retention period of any record in the system.

7. Disposition Pending Status. "Disposition pending" means that all affected records must be kept in the active file until NARA issues final disposition instructions, per Reference a. Retain records as "permanent" until NARA prescribes specific disposition instruction.

8. Damage To or Unauthorized Disposition of Records. Unauthorized disposition is the removal from NORAD and USNORTHCOM custody or the destruction of records without regard to the approved NARA disposition schedules.

8.1. Any person or activity having knowledge of impending, actual, or threatened unlawful removal, defacing, alteration, or destruction of records must notify the CRM immediately by memorandum.

8.2. RO/FCs must make a reasonable effort to salvage, restore, or reconstruct records lost, damaged, or destroyed before approved disposition dates. RO/FCs must identify the records in a memorandum to the CRM. At a minimum, include:

8.2.1. Title or description of records, dates of records, classification, applicable disposition series and volume of records lost or destroyed. If lost/destroyed records were in paper format, loss shall be expressed in linear inches.

8.2.2. Cause of the loss or destruction, if known.

8.2.3. Recovery or reconstruction action, if any

8.2.4. Steps taken to prevent instance from reoccurring again in future.

8.2.5. Additional information that will make the report more meaningful.

8.3. The case shall be kept in an "open" status until a copy of the final disposition report is received from the CRM.

8.4. Ensure the SF 135, Records Transmittal and Receipt, reflects an accounting for lost or destroyed records that cannot be reconstructed. Attach a copy of the report and a copy of the SF 135, in lieu of the lost or damaged record, at the time of retirement.

8.5. Penalties for damage to or Unauthorized Disposition of Records.

8.5.1. Actions to willfully and unlawfully conceal, remove, mutilate, obliterates, destroy, or attempts to do so, with intent to do so, can subject the individual(s) to criminal liability (18 U.S.C. § 2071).

9. Shipping or Transferring Records. SF 135, Records Transmittal and Receipt, will be used to transfer or ship any records to any other function, organization, or agency. When a function is transferred from one organization to another, the current files (including electronic files) relating to the transferred function must be forwarded to the gaining element. The inactive files of the transferring office must be transferred to the appropriate records center in coordination with the CRM.

9.1. Transfer within NORAD and USNORTHCOM. Send to the CRM, a complete list of the active records transferred to the gaining organization and any SF 135 listing inactive files previously transferred. Both organizations must submit for approval an updated File Plan, including/removing the related record series.

9.2. Transfer outside NORAD and USNORTHCOM. Transferring records, including electronic records, outside NORAD and USNORTHCOM requires the CRM and gaining CRM/ROs approval. Submit a completed SF 135 to include an index or listing of records being transferred.

10. Destruction of Records. Directorates and Special Staff will ensure proper management and destruction of material, to ensure valuable information is not improperly disposed of, and that such destruction of Command records is done according to laws pertaining to the destruction of official records (any papers, books, photos, final briefings or other material which documents official actions, decisions, policies or procedures). This is of primary concern for items presented for shredding.

10.1. Ensure that any and all destruction of material is considered to be non-record material. Any one or more of three factors below determines whether something is a non-record. These factors are:

10.1.1. Nature of the Material: Some items by their very nature are non-records. They include blank versions of forms, routing sheets, transmittal sheets, etc.

10.1.2. Relationship to Records: Material such as working papers and drafts that are used in creating official records are non-record. Identical duplicates of all records maintained in the same file are non-record. Follow-up materials, such as suspense copies of correspondence, that are used to facilitate operations, but not to document those operations, are non-records.

10.1.3. Use of the Material: Materials used exclusively for reference purposes are non-record. Copies of records maintained solely for reference purposes are also non-record if no administrative action is taken on them.

11. Waivers. Waivers or deviations from this directive are at the discretion of the Chief of Staff. Substantial justification for non-compliance with this instruction must exist before a waiver request will be considered.

CHARLES D. LUCKEY, MG, USA
Chief of Staff

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

5 U.S.C. *§* 552a, *Privacy Act*

18 U.S.C. § 2071

44 U.S.C. *§* 3301

Title 36, Code of Federal Regulations, Chapter XII, *National Archives and Records Administration*; Subchapter B, *Records Management*

CJCSI 3231.01, (S) *Safeguarding the Single Integrated Operational Plan* (U*),* 6 Jun 2007

CJCSI 5760.01 - *Records Management Policy for the Joint Staff and Combatant Commands,* 13 Jul 2009

CJCSI 5714.01D - *Release Procedures for Joint Staff and Joint Papers and Information,* 18 Apr 2012

CJCSM 5760.01A, *The Joint Staff and Combatant Command Records Management Manual*: *Volume I – Procedures,* 13 July 2009

CJCSM 5760.01A, *The* Joint *Staff And Combatant Command Records Management Manual*: *Volume II--Disposition Schedule,* 13 July 2012

DOD 5200.1-R, *Information Security Program Regulation,* 9 Oct 2008

DOD 5400.11-R - *Department of Defense Privacy Program,* 14 May 2007

AFI 33-332 - *Air Force Privacy Act Program,* 16 May 2011

(C) *United States Implementation of NATO Security Procedures* (U), 1982

Adopted Forms

JS Form 31, *Joint Staff/Combatant Command List of Selected File Numbers*

JS Form 32, *Joint Staff/Combatant Command Records Management Inspection List*

SF Form 135, *Records Transmittal and Receipt*

Abbreviations and Acronyms

CDR—Commander, NORAD and USNORTHCOM

CJCS—Chairman, Joint Chiefs of Staff

CJCSI—Chairman, Joint Chiefs of Staff Instruction

CJCSM—Chairman, Joint Chiefs of Staff Manual

COOP—Continuity of Operations

CRM—Command Records Manager

DOD—Department of Defense

DPCLO—DOD Privacy and Civil Liberties Office

DVO—Destruction Validation Officer

EIS—Electronic Information System

ERMA—Electronic Records Management Application (a.k.a. Records Repository)

FC—Files Custodian

FOIA—Freedom of Information Act

FRC—Federal Records Center

HO—Command Historian

IAW—in accordance with

IT—Information Technology

JIOC—Joint Intelligence Operations Center

JS—Joint Staff

MEF— Mission Essential Functions

NARA—National Archives and Records Administration

NATO—North Atlantic Treaty Organization

NORAD—North American Aerospace Defense

O&M—Operations and Maintenance

OCR—Optical Character Recognition

OPR—Office of Primary Responsibility

PAO—Privacy Act Officer

PII—Personally Identifiable Information

RO—Records Officer

SAV—Staff Assistance Visit

SCI—Specially Controlled Information

SF—Standard Form

SIOP—Single Integrated Operation Plan

U.S.C.—United States Code

USNORTHCOM—United States Northern Command

Definition of Terms

Disposition—(1) The actions taken regarding records no longer needed in current office space. These actions include transfer to agency storage facilities or Federal Records Centers, transfer from one Federal agency to another, transfer of permanent records to the National Archives and Records Administration, and disposal of temporary records. (2) The actions taken regarding non-record materials when no longer needed, including screening and destruction (in accordance with the Records Disposition Schedule).

Disposition Schedule—A document providing authority for the final disposition of records. Also called records disposition schedule, records control schedule, records retention schedule, or schedule. NARA is the approval authority for all Federal schedules.

File Plan—A plan designating the physical and/or electronic location(s) at which an agency's files are to be maintained, the specific types of files to be maintained there and the organization element(s) having custodial responsibility. Also a document containing the identifying number, title or description, and disposition authority of files held in an office.

Files Custodian—Position designated by the Director/Lead responsible for the physical custody, maintenance, and disposition of records in an office-of-record. There may be more than one office-of-record and corresponding Files Custodians within a directorate.

Federal Records Center—A records center operated by NARA that is authorized to store Federal records on a reimbursable basis.

Inactive Records—Records in a retention period after the cutoff date and awaiting final disposition as approved by NARA.

Inventory—A survey of agency records and non-record materials conducted primarily to develop records schedules and to identify various records management problems.

Non-record—Information materials that are not part of the legal definition of a record. May include routing slips, transmittal sheets, and blank forms; reading file and suspense copies of correspondence; materials concerning fringe activities of the agency such as employee charitable activities; and physical exhibits, artifacts, and material objects having no documentary value.

Office of Record—An office designated by the Director for the custody, maintenance, and retirement or disposal of the records it holds.

Permanent Records—Records appraised by NARA as having enduring value because they document the organization and functions of the agency that created or received them and/or because they contain significant information on persons, things, problems, and conditions which the agency dealt with.

Personal Papers—Papers created solely at the discretion and for the convenience of the author, not as a part of JS/Combatant Commander official records preserved as evidence of decisions and policies.

Records—"All books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference and stocks of publications and of processed documents are not included." (Title 44 U.S.C. 3301)

Record Copy—The official or file document you so mark and recognize, complete with enclosures and related papers. The file copy created by the action office, complete with coordination, enclosures, or papers related to the action. Such copies are to be specifically identified as the record copy by the creating office.

Record Disposition—See Disposition.

Record Disposition Schedule—See Disposition Schedule.

Series of Records—A group of records with an identical disposition standard approved or pending approval by NARA, identified by a specific number in CJCSM 5760.01A, Vol. II. A series of records may be further broken down and have different disposition standards based on their location (at the headquarters of an organization as opposed to those at a subordinate unit); use (record copy versus reference copy); or because of a Federal law or court decision.

Attachment 2

SAMPLE RO/FC/DVO APPOINTMENT LETTER

NORTH AMERICAN AEROSPACE DEFENSE COMMAND
AND
UNITED STATES NORTHERN COMMAND

Date

MEMORANDUM FOR N-NC/CSR
ATTN: Command Records Manager

FROM: [Directorate]

SUBJECT: Records Officer, Files Custodian and Destruction Validation Officer Appointment

1. The following members are appointed as the Primary/Alternate Records Officer:

Name Grade/Rank Room Phone#
Primary/Alternate

2. The following member is appointed as the Files Custodian:

Name Grade/Rank Room Phone#
Office of Record

3. The following member is appointed as the Destruction Validation Officer:

Name Grade/Rank Room Phone#

4. Questions can be directions to [POC] at [XXX-XXXX].

[Director's Signature Block]

Courtesy copy:
[Appointees identified in this memo]

Attachment 3

RECORDS INVENTORY WORKSHEET

Records Inventory Worksheet

Directorate	**Office Symbol:**	**Name:**			**Bldg/Room #**	**Date**
Type/Title:	**Description** *(Brief – no more than two sentences)*	**Purpose:**	**Frequency:**	**Media Format** (*Paper, Electronic, Microfilm, Publication, Book , Video, Audio, Other –list)***:**	**Filing *Method*** *(Alphabetical Chronological Geographical, etc.):*	**Record Characteristic** (PII, Vital Record)**:**

Attachment 4

ELECTRONIC INFORMATION SYSTEM (EIS) QUESTIONNAIRE

NORAD and USNORTHCOM Electronic Information System (EIS) Questionnaire

DATE:	
SYSTEM NAME:	SYSTEM'S ACRONYM, IF APPLICABLE
ALSO KNOWN AS – NAMES AND ACRONYMS	FORMERLY KNOWN AS - NAMES AND ACRONYMS

CONTACT INFORMATION

OFFICE THAT OWNS OR IS RESPONSIBLE FOR THE SYSTEM:		
CONTACT NAME:	PHONE NUMBER:	ROLE:
CONTACT NAME:	PHONE NUMBER:	ROLE:

SYSTEM GENERAL INFORMATION

BRIEFLY DESCRIBE THE SYSTEM, ITS FUNCTION AND PURPOSE:

WHAT NORAD and USNORTHCOM PROGRAM OR MISSION IS SUPPORTED BY THE SYSTEM?

IS THE SYSTEM

□ An existing system?	□ A system in its development stages?	□ An obsolete system?
Date system implemented:	Planned implementation date:	Date range system was active:

WHAT IS THE SYSTEM'S SECURITY CLASSIFICATION?

□ UNCLASSIFIED □ FOUO □ CONFIDENTIAL □ SECRET □ TOP SECRET □ TS SCI

WHAT IS THE SYSTEM'S HARDWARE AND SOFTWARE ENVIRONMENT?
For example, is the system a commercial off-the-shelf (COTS) software product, an Oracle or Access database

HAS A PRIVACY IMPACT ASSESSMENT BEEN PREPARED FOR THE SYSTEM?
□ No □ Yes If YES, enter the record series number of the document:

DOES THE SYSTEM HAVE A USER MANUAL OR OTHER DOCUMENTATION?

□ No □ Yes If YES, enter the record series number of the document:

LIST ANY WEBSITE ADDRESS(ES) THAT MAY ASSIST IN LEARNING ABOUT YOUR SYSTEM

IN YOUR OPINION, HOW LONG IS THE DATA IN THE SYSTEM OF VALUE TO NORAD and USNORTHCOM?

□ Less than 3 years □ 3 to 10 years □ Longer than 10 years

SYSTEM DATA AND WORKFLOW

SUMMARIZE PROCESS AND WORKFLOW OF HOW INFORMATION IS ENTERED INTO AND USED IN THE SYSTEM

BRIEFLY DESCRIBE DATA (OR OTHER INFORMATION SUCH AS A SCANNED IMAGE) ARE INPUT (ENTERED) INTO THE SYSTEM, INCLUDING WHO ENTERS THE DATA/INFORMATION AND HOW

DOES THE DATA ENTERED INTO THE SYSTEM COME FROM ANY OTHER SYSTEM(S)?

□ No □ Yes If YES, identify the system(s):

WHAT HAPPENS TO DATA/INFORMATION IN THE SYSTEM?

For example, is the data migrated into another system or used by any other systems? Is the data/information output in the form of correspondence, a report, or graph?

IS THE INFORMATION FROM THE SYSTEM RECORDED IN ANOTHER SYSTEM OF RECORDS?

□ No □ Yes If YES, identify the system(s):

IDENTIFY ANY TYPE OF METADATA THAT IS CAPTURED IN THE SYSTEM

(Metadata is “data about the data” which is typically information the system is programmed to capture, such as the time/data when an entry was made into the system, information on who entered the data, etc.)

SYSTEM BACK-UPS AND AUDIT

DESCRIBE THE TYPE OF SYSTEM BACK-UPS THAT OCCUR, SUCH AS FULL OR INCREMENTAL

DESCRIBE THE FREQUENCY OF BACK-UPS

WHAT TYPE OF SYSTEM AUDITING IS CONDUCTED?

Attachment 5

VITAL RECORDS AND INFORMATION QUESTIONNAIRE

Vital Record/Information Questionnaire

Date:

Organization/Location:

Organization/Location POC Name:

Organization/Location POC Number/e-mail:

1. Explain, in “laymen’s terms”, what does your office do?

2. Is there anything that your office does that you would consider to be critical to the organization?

3. Briefly describe the types of records or other information your office creates.

4. Do you consider any of these records to be invaluable – meaning their loss or unavailability during an emergency would result in catastrophic effect on your organizations mission or operations?

5. If any of these records are critical, provide the following:

   a. Records Bucket (Record Series) Title:

   b. Media Format:

   c. How **soon** would you need access to the Record(s)? (hours, days, weeks)

   <u>Purpose of the Vital Record or Information</u>:

   ◊ Needed for continuing operations during the disaster? If so, how is it used?

   ◊ Needed after the disaster or emergency to protect legal rights and financial or other interests of your organization? If so, how is it used?

   ◊ Record or Information is both “emergency planning” and “legal and financial rights & interests.”

6. If you have vital records or information, how are you protecting them now?

7. If you have vital records or information, how are you ensuring that they stay current and are available during an emergency?

8. If you have vital records or information, are you considering an emergency in which you may not have access to NORAD and USNORTHCOM networks or repositories?