BY ORDER OF THE COMMANDER
UNITED STATES TRANSPORTATION COMMAND

USTRANSCOM INSTRUCTION 31-02
6 APRIL 2018

Security

SECURITY CLASSIFICATION GUIDE

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available electronically on the USTRANSCOM electronic library.

RELEASABILITY: There are no releasability restrictions on this publication

OPR: TCJ3-MP
Approved By: TCJ3 (Maj Gen Ricky Rupp)
Supersedes: USTRANSCOMI 31-02, 09 Oct 2015
Pages: 34
Distribution: e-Publishing

This Instruction provides the policies and procedures for implementing Department of Defense (DOD) Manual 5200.01, *DOD Information Security Program*, Volumes 1-4, and is issued under the authorities contained in Executive Order 13526, DODM 5200.01, and Part IV, National Archives and Records Administration, Information Security Oversight Office, 32 CFR Parts 2001 and 2004, *Classified National Security Information (Directive No. 1); Final Rule*. It provides guidance on the classification of information pertaining to the United States Transportation Command (USTRANSCOM). It applies to all USTRANSCOM military, civilian, and contractor personnel; the Joint Transportation Reserve Unit (JTRU), the Military Surface Deployment and Distribution Command (SDDC), and the Joint Enabling Capabilities Command (JECC). It does not apply to the Air Mobility Command (AMC) and the Military Sealift Command (MSC) as they have their own Original Classification Authority (OCA). Failure to observe mandatory provisions of this Instruction by military personnel is a violation of Article 92, Uniform Code of Military Justice. Violation by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Refer recommended changes and questions about this publication to the office of primary responsibility using Air Force Form 847, *Recommendation for Change of Publication*. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with USTRANSCOM Instruction 33-32, *Records Management*.

SUMMARY OF REVISIONS.

The following changes have been made: changed all references from TCJ3-F to TCJ3-M, from TCJ3-FP to TCJ3-MP; changed approved and signature block from VADM Brown to Maj Gen Rupp; added USTRANSCOM Chief of Staff (TCCS) as an acting Original Classification Authority (OCA) in the absence of the Commander; added Foreign Entity Vetting (FEV) items; changed date of declassification in all items from "date 25 years from date of original classification" to "date 25 years from creation date;" added multiple items of information in the classification matrices and included two new items pertaining to agreements with countries in Attachment 8.

1. References and Supporting Information. References, related publications, abbreviations, acronyms, and terms used in this instruction are listed in Attachment 1.

2. General Guidance.

2.1. The guidance contained in this Instruction pertains to information and compiled data in USTRANSCOM systems that are originally classified by a USTRANSCOM Original Classification Authority (OCA).

2.2. All originally classified decisions in USTRANSCOM must be recorded and are subject to inspection by the Information Security Oversight Office (ISOO). Originally classified decisions are also reported to the DOD Directorate of Security Policy & Oversight on an annual basis. The specific format for recording originally classified decisions is at the determination of the OCA or his/her executive staff.

2.3. Only Commander, USTRANSCOM (TCCC), Deputy Commander, USTRANSCOM (TCDC), Director of Operations (TCJ3), Director of Strategic Plans, Policy, and Logistics (TCJ5/J4), and Director of Command, Control, Communications, and Cyber Systems (TCJ6) have original classification authority. The Chief of Staff (TCCS) has OCA in the absence of TCCC. Original classification authority may not be delegated. See Paragraph 3 (Roles and Responsibilities) of this instruction for OCA designation.

2.4. Classification guides for specific systems, plans, programs, or projects have precedence over this instruction for the affected system, plan, program or project classification decisions.

2.5. All unclassified information must be thoroughly reviewed before release in accordance with USTRANSCOM Instruction 33-26, *Freedom of Information Act (FOIA) Program*.

2.6. Information not marked Releasable to (REL TO) must be submitted to the USTRANSCOM Foreign Disclosure Officer before release is authorized to non-US personnel working in USTRANSCOM.

2.7. Individuals with the appropriate security clearance, who are required by their duties to derive classified source information from other sources or security classification guides, may only do so if they have been trained on derivative classification (located in the training management system) within the past two years.

2.8. The original classification authority will classify information that:

2.8.1. Is one of the eight categories for classification as stated in section 1.4 of Executive Order 13526.

2.8.2. Reveals an association to one of the categories in section 1.4 of Executive Order 13526 when compiled, as stated in section 1.7 of Executive Order 13526.

2.9. Notify TCJ3-MP immediately if in possession of suspected inappropriately classified or inappropriately unclassified information.

2.10. When a source document's declassification date is marked with Originating Agency's Determination Required (OADR), the derivative declassification marking shall be a calculated date that is 25 years from the date of the document's origin unless other guidance is available from the OCA.

2.11. Information papers, briefings, memorandums, after action reports, etc., based on derivatively classified information, are overall classified at the highest level of the derivatively classified information contained in the document.

2.12. Derivatively classified information (i.e., originally classified by an original classification authority outside of USTRANSCOM) maintains that level of classification unless information has been improperly classified. Challenges to the classification level must be coordinated with TCJ3-MP.

2.13. Special materials such as overlays and graphic displays containing classified information must be marked with the highest classification of the information on the overlay/display as well as the declassification guidance.

2.14. Security classification guidance for communications security information or material applicable to or used in support of the National Military Command System (NMCS), as well as cryptographic equipment, is under the purview of the National Telecommunications and Information Systems Security Committee.

2.15. The determination of security classification for subscriber communications equipment employed in support of the USTRANSCOM mission, or its subsystems, resides with the supporting Service or Defense agency.

2.16. Include portion markings, overall classification in the banner lines, the source of the classification, and the declassification date in all classified emails.

2.17. FOR OFFICIAL USE ONLY is not a classification of information. It is a dissemination control marking used with UNCLASSIFIED information. DOD policy does allow for FOR OFFICIAL USE ONLY to be used by itself in banner lines (i.e. the top and bottom overall marking) although the preferred method is to use the classification marking with the dissemination control marking stated as UNCLASSIFIED//FOR OFFICIAL USE ONLY. In documents with this information, applicable portion marking are marked as (U//FOUO).

2.18. Application of FOR OFFICIAL USE ONLY as a dissemination control marking may be applied when disclosure to the public of that particular record, or portion thereof, would reasonably be expected to cause foreseeable harm to an interest protected by one or more of the Freedom of Information Act (FOIA) exemptions 2-9. It is the responsibility of the document's originator to determine at origination whether the information may qualify for FOR OFFICIAL USE ONLY status and to ensure the marking is applied as required. The dissemination control marking does not automatically mean the information is qualified for exemption. Questions on application of FOR OFFICIAL USE ONLY can be forwarded to TCJ3-MP.

3. Roles and Responsibilities.

3.1. TCCC:

3.1.1. Serve as a Top Secret and below OCA**.**

3.2. TCDC:

3.2.1. Serve as a Top Secret and below OCA.

3.3. TCCS:

3.3.1. Serve as a Secret and below OCA when officially designated to assume the duty position of TCCC or TCDC in an acting capacity during their absence.

3.4. TCJ3:

3.4.1. Serve as a Secret and below OCA.

3.5. TCJ5/J4:

3.5.1. Serve as a Secret and below OCA.

3.6. TCJ6:

3.6.1. Serve as a Secret and below OCA.

3.7. TCJ2 Foreign Disclosure Officer (FDO):

3.7.1. Approve/Disapprove all classified and controlled unclassified information proposed for release to official representatives of foreign governments or recognized international coalitions in accordance with National Disclosure Policy (NDP-1); Intelligence Community Directive (ICD) 403; Director of Central Intelligence Directive DCID 6/6 *Security Controls on the Dissemination of Intelligence Information and* 6/7 *Intelligence Disclosure Policy;* Chairmen Joint Chief of Staff Instruction (CJCSI) 5221.01D *Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations;* and USTRANSCOM Instruction 14-8 *Security Classification Markings – Authorization for Release To (REL TO) and Dissemination Control/Declassification Markings*.

3.7.2. Review all requests for dissemination of classified information to Foreign Exchange or Liaison Officers in USTRANSCOM.

3.8. TCJ3-MP:

3.8.1. Receive updates for items of information to be added or subtracted to the classification matrix.

3.8.2. Provide guidance on classification and classification markings.

3.8.3. Comply with provisions of DOD information security policy for Security Classification Guides on periodic reviews and submission to the Defense Technical Information Center for placement into the DOD Index of Security Classification Guides (SCG).

3.8.4. Resolve all conflicts involving discrepancies between this and any other SCG.

3.9. Coordinating Instructions.

3.9.1. Comply with the parameters set forth in this SCG.

3.9.2. Alert TCJ3-MP as to discrepancies between this and any other SCG.

4. Compilation of Information. The compilation of individually unclassified information may, at times, require classification if the compiled information reveals an additional association or relationship that (1) meets the standards for classification, and (2) is not otherwise revealed in the individual items of information. Compilation is an aggregation of pre-existing unclassified items of information. Additionally, whenever the reason for classification is not apparent from the content of the information, the Original Classification Authority shall provide a more detailed explanation of the reason for classification. It is possible to have a classified document in which all the individual portions are unclassified. The compilation of the unclassified information reveals an association or relationship not otherwise evident when the portions are used individually and the application of required classification markings are warranted.

5. Classification Matrix. A copy is provided in Attachments 3-15.

5.1. Information To Be Protected Column**.** The "INFORMATION TO BE PROTECTED" column states precisely the elements of information to be protected using categorization to the extent necessary to ensure the information can be readily located.

5.2. Classification Column**.** The "CLASS" column states which classification level applies to each element of information listed under the "INFORMATION TO BE PROTECTED" column. The markings listed below are accompanied by descriptive extracts from DODM 5200.01, Volume 1.

5.2.1. TS - TOP SECRET. This classification is applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

5.2.2. S - SECRET. This classification is applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

5.2.3. C - CONFIDENTIAL. This classification is applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

5.2.4. U - UNCLASSIFIED. Information with this marking is unclassified. However, selected controlled unclassified information (CUI) requires additional protections. CUI has been included in this classification guide for the purpose of assisting USTRANSCOM personnel determine that it is unclassified.

5.3. Related System, Plan, Program or Project Column. This column notes the related System, Plan, Program or Project as identified in Attachment 2.

5.4. Reason. The "REASON" column specifies the reason for classification, citing the appropriate category of information listed in Section 1.4 of Executive Order 13526 as follows:

5.4.1. 1.4(a) – Military plans, weapons systems, or operations.

5.4.2. 1.4(b) – Foreign government information.

5.4.3. 1.4(c) – Intelligence activities (including special activities), intelligence sources or methods, or cryptology.

5.4.4. 1.4(d) – Foreign relations or foreign activities of the United States, including confidential sources.

5.4.5. 1.4(e) - Scientific, technological, or economic matters relating to the national security.

5.4.6. 1.4(f) – United States Government programs for safeguarding nuclear materials or facilities.

5.4.7. 1.4(g) – Vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security.

5.4.8. 1.4(h) – Weapons of mass destruction.

5.5. Declassify On Column**.** The "DECLASSIFY ON" column specifies the date or event for declassification of the information. There are various standards to be applied when determining the declassification date. The first standard is whether the information was originally classified by someone outside of USTRANSCOM. In this situation the declassification date will be set by the original classifying authority and all USTRANSCOM use of that information will include the derived declassification date (i.e., use the date to declassify that came with the originally classified source). For information originally classified by a USTRANSCOM Original Classification Authority, the following declassification periods will be selected based on the sensitivity of the information in accordance with Section 2001.12 of ISOO Directive No. 1:

5.5.1. A date or event less than 10 years from the date of the document; or if unable to identify such a date or event:

5.5.2. A date 10 years from the date of the document.

5.5.3. A date greater than 10 years but less than 25 years from the date of the document.

5.5.4. A date 25 years from the date of the document.

5.5.5. Source documents marked X1 through X8. The use of X1 through X8 markings are prohibited after 22 September 2003. Therefore, no originally classified information in USTRANSCOM after the above date shall bear these markings as the declassification dates. When derivatively classifying information from an originally classified document with the X1 through X8 declassification markings, USTRANSCOM personnel will follow the 16 February 2007 guidance issued by the Director of ISOO, stating the derivative use of the X1 through X8 markings which were on documents prior to 22 September 2003 shall be marked with a "Declassify On" date of September 2028, absent further guidance from the originating Original Classification Authority.

5.5.6. No USTRANSCOM documents will be originally marked with declassification instructions stating Originating Agency Determination Required (OADR).

5.6. Remarks. The "REMARKS" column contains any other pertinent information for each element of information, as appropriate, to include downgrading instructions.

6. Release of Classified Information. The term "release" includes, but is not limited to, any technical data, articles, speeches, photographs, brochures, advertisements, presentations, and displays.

6.1. To Other Government Agencies. Classified information will only be released to other government agencies when the following has been obtained: verification of the clearance level of the receiver and verification that the receiver has a valid need-to-know. It is the responsibility of the individual releasing the information to verify these considerations before any classified is released.

6.2. To Foreign Nationals. Classified and controlled unclassified information will not be released to foreign nationals without FDO review and approval. The only classified information that is releasable is that information specifically marked as REL TO and then includes the countries to which authorized release has been approved by the FDO. Only the TCCC and FDO have the authority to add or modify the REL TO makings on USTRANSCOM data. Additionally, the FDO will coordinate for the release of classified data for OCAs that reside outside of USTRANSCOM. Coordinate all requests for release of information with the USTRANSCOM Foreign Disclosure Officer.

6.3. Public Release of UNCLASSIFIED Information. Releases of UNCLASSIFIED information pertaining to the USTRANSCOM mission will not be made available to the public or to uninvolved United States Government (USG) agencies, Non-Governmental Organizations (NGOs), or foreign agencies without the prior approval of USTRANSCOM Public Affairs and/or affected organizational element(s). Official DOD information intended for public release must be reviewed for clearance in accordance with DOD Instruction 5230.29, *Security and Policy Review of DOD Information for Public Release*. **It is imperative that all information be processed through official security review channels since information may not be reclassified once it has been declassified and released to the public under proper authority.** The Freedom of Information Act provides a means for the public to request information from the

US Government (see USTRANSCOM Instruction 33-26).

7. Declassification and Downgrading. Information requiring classification protection will remain classified per the original classification authority declassification marking. When a document or item of material is marked for downgrading or declassification on a date or event, the downgrading or declassification is automatic at the specified time unless word to the contrary has been received from the originator or other authority. If the holder of the material has reason to believe it should not be downgraded or declassified, he or she shall notify the originator through appropriate administrative channels. The document or material shall continue to be protected at the originally assigned level of classification until the issue is resolved.

RICKY N. RUPP
Major General, USAF
Director of Operations

15 Attachments.
1. Glossary of References, Abbreviations, Acronyms and Terms
2. System, Plan, Program or Project Classification Matrix
3. Manpower and Personnel (TCJ1) Classification Matrix
4. Intelligence (TCJ2) Classification Matrix
5. Operations (TCJ3) Classification Matrix
6. Security (Information, Personnel, Industrial, Physical) and Antiterrorism (TCJ3-M) Classification Matrix
7. Information Operations (TCJ3-MI) Classification Matrix
8. Strategic Plans, Policy and Logistics (TCJ5/J4) Classification Matrix
9. Command, Control, Communications, and Cyber Systems (TCJ6) Classification Matrix
10. Financial Information Operations (TCJ8) Classification Matrix
11. Acquisition Information (TCAQ) Classification Matrix
12. Inspector General (TCIG) Classification Matrix
13. Public Affairs (TCPA) Classification Matrix
14. Historical Information (TCRC) Classification Matrix
15. Senior Personnel Travel/Meeting Conferences Classification Matrix

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Executive Order 13526, 29 December 2009, *Classified National Security Information.*
Information Security Oversight Office Directive No. 1, *Marking National Classified Security Information.*
CJCSI 5221.01 D, Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations.
DCIDS 6/6 *Security Controls on the Dissemination of Intelligence Information.*
DCIDS 6/7, Intelligence Disclosure Policy.
DISA Circular 300-115-3, 1 June 2013, *Communications Security.*
DOD Instruction 5230.29, Security and Policy Review of DOD Information for Public Release.
DODI 5400.11, *DOD Privacy Program.*
DODM 5200.01, Volume 1, *DOD Information Security Program: Overview, Classification, and Declassification.*
DODM 5200.01, Volume 2, *DOD Information Security Program: Marking of Classified Information.*
DODM 5200.01, Volume 3, *DOD Information Security Program: Protection of Classified Information.*
DODM 5200.01, Volume 4, *DOD Information Security Program: Controlled Unclassified Information.*
National Security Telecommunications and Information Systems Security Instruction (NSTISSI).
USTRANSCOM Instruction 33-32, Records Management.
USTRANSCOM Instruction 33-26, Freedom of Information (FOIA) Program.
USTRANSCOM Pamphlet 14-8, Security Classification Markings – Authorization for Release To (REL TO) and Dissemination Control/Declassification Markings.

Abbreviations and Acronyms

AMW- Airlift Mobility Wing
APOD/SPOD – Aerial/surface Port of Debarkation
CBRNE – Chemical, Biological, Radiological, Nuclear and High-yield Explosives
CMI – Classified Military Information
COOP – Continuity of Operations
CRAF – Civil Reserve Airlift Fleet
CUI – Controlled Unclassified Information
DISA – Defense Information Systems Agency
DOD – Department of Defense
DRSN – Defense Red-switched Network
FDO – Foreign Disclosure Officer
FOIA – Freedom of Information Act
FPCON – Force Protection Condition
GOC – Global Operations Center
IAW – In accordance with
ISOO – Information Security Oversight Office
JECC – Joint Enabling Capabilities Command
NMCS – National Military Command System
NIPR – Non-classified Internet Protocol Router
OADR – Originating Agency Determination Required
OCONUS – Outside the Continental United States
POTUS/VPOTUS – President/Vice President of the United States

REL TO – Authorized for Release to
SAAM – Special Assignment Airlift Mission(s)
SIPR – Secret Internet Protocol Router
TCCC – Commander, USTRANSCOM
TCCS – Chief of Staff, USTRANSCOM
TCDC – Deputy Commander, USTRANSCOM
TCJ3 – Director, Operations and Plans, USTRANSCOM
TCJ5/J4 – Director, Strategic Plans, Policy, and Logistics, USTRANSCOM
TCJ6 – Director, Command, Control, Communications and Cyber Systems, USTRANSCOM
TPC – two person control
USG – United States Government
USTRANSCOM – United States Transportation Command
VISA – Voluntary Intermodal Sealift Agreement

Attachment 2

SYSTEM, PLAN, PROGRAM OR PROJECT CATEGORIES

Official Title	**Category: System, Plan, Program or Project**	**Description**	**Functional OPR(s)**
AT21	Program/System	Agile Transportation for the 21st Century	TCJ3
JFAST	Program/System	Joint Flow and Analysis System for Transportation	TCJ3
TransViz	Program/System	Transportation Visualizer	TCJ3
AMP	Program/System	Analysis of Mobility Platform	TCAC
SMS	Program/System	Single Mobility System	TCJ3
IGC	Program/System	Integrated Data Environment/Global Transportation Network Convergence	TCJ3
CAMPS	Program/System	Consolidated Air Mobility Planning System	HQ AMC/A3; TCJ3
Logbook	Program/System	Commentary on linked tasks	TCJ3
DRRS	Program/System	Defense readiness information	TCJ3
TRAC2ES	Program/System	Patient evacuation system	TCSG
JOPES	Program/System	Joint Operation Planning and Execution System	TCJ3

Attachment 3

MANPOWER AND PERSONNEL (TCJ1) CLASSIFICATION MATRIX

Information To Be Protected	Classification	Related System, Plan, Program or Project	Reason	Declassify On	Remarks
Overall force structure with total personnel strength with percentage of personnel fills	C		1.4(g)	Date 10 years from original classification	Total listing of all forces is classified. Individual unit strength is unclassified
Manning rosters	U		N/A	N/A	No SSN on rosters
Leave schedules, location of key personnel on leave	U		N/A	N/A	
Key personnel shortages	U		N/A	N/A	
Personnel Accountability Recall System (PARS) data	U		N/A	N/A	

Attachment 4

INTELLIGENCE (TCJ2) CLASSIFICATION MATRIX

Information To Be Protected	Classification	Related System, Plan, Program or Project	Reason	Declassify On	Remarks
USTRANSCOM Threat Working Group briefings	See remarks			Declassify date from sources	All derivatively classified portions are marked IAW the source document classification markings
USTRANSCOM developed threat analyses	S		1.4(c)	Date 25 years from the date of creation	Portions containing derivatively classified information are marked IAW the source document classification markings
USTRANSCOM Intelligence estimates	S – TS		1.4(c)	Date 25 years from the date of creation	Portions containing derivatively classified information are marked IAW the source document classification markings
USTRANSCOM Intelligence Requirements (IRs)	U – TS		1.4(c)	Date 25 years from the date of creation	IRs are classified C-TS with a dissemination control of either

					NOFORN or REL TO USA, FVEY
USTRANSCOM Commander's Critical Information Requirements (CCIR)	U – S		1.4(c)	Date 25 years from the date of creation	CCIR's are initially unclassified but become Secret when filled in with supporting information
Essential Elements of Friendly Information (EEFI)	S		1.4(g)	Date 25 years from the date of creation	

Attachment 5

OPERATIONS (TCJ3) CLASSIFICATION MATRIX

Information To Be Protected	Classification	Related System, Plan, Program or Project	Reason	Declassify On	Remarks
Locations of CONUS strategic seaports and airfields	U		N/A	N/A	
Locations of OCONUS strategic seaports and airfields	U		N/A	N/A	
Out-load capabilities of CONUS strategic commercial seaports	U//FOUO		N/A	N/A	Dissemination control marking of FOR OFFICIAL USE ONLY applied based on FOIA exemption 5
USTRANSCOM OPORDS, OPLANS, Contingency Plans	U – TS		1.4(a)	Date 25 years from date of original classification	Force movements linked to specific OPORDs and/or OPLANs become classified to level of OPORD or OPLAN
Security posture and plans, and security provided for lift assets, ports, routes and infrastructure	S		1.4(a)	Date 25 years from date of original classification	
Patient movements with or without routes or movement schedules	U		N/A	N/A	
Distribution information	U//FOUO		N/A	N/A	

containing lift asset schedules, movement dates/times, routes, passenger and cargo manifest details					
USTRANSCOM support to countries needing assistance resulting from natural disasters	U		N/A	N/A	
POTUS and VPOTUS missions	S		1.4(a)	Date 30 days from date of mission completion	
USTRANSCOM support to Homeland Defense and emergencies	S		1.4(a)	Date one year from date of completion of support	
USTRANSCOM support to natural disasters relief efforts	See remarks			Date derived from classified source	Unclassified unless directive to USTRANSCOM is classified, and then only the portions marked as classified are classified
Security at DOD piers on commercial ports for military operations	C		1.4(a)	Date 10 years from creation	
USTRANSCOM GOC battle rhythm	U		N/A	N/A	
SAAMS validations	U		N/A	N/A	
USTRANSCOM developed exercises	U		N/A	N/A	
Ready Reserve fleet ship status; operational capability	U		N/A	N/A	

USTRANSCOM participation in 375th AMW exercises	U		N/A	N/A	
USTRANSCOM exercises lessons learned	U		N/A	If including classified from a derived source, declassification date is as stated in source	Some portions may be classified if deriving from a classified source

Location of USTRANSCOM and JECC COOP. Any of the following elements when combined with the word COOP or alternate site: address; city; building number or name; or description indicators including server location	S		1.4(a)	Date 25 years from date of original classification	No placing of single location indicators such as the COOP phone numbers on unclassified share point pages
USTRANSCOM support for DOD CBRNE events	S		1.4(a)	Date 25 years from date of original classification	
Vulnerabilities at commercial APODS or SPODS with respect to DoD operations	S		1.4(g)	Date 10 years from determination	
USTRANSCOM directives pertaining to activation of CRAF or VISA	S		1.4(a)	Date 10 years from date of activation	
USTRANSCOM courier movements stating two-person control	C		1.4(a), 1.4(c), 1.4(f), 1.4(h)	Immediately after completion of movement	
USTRANSCOM courier movements not using the words “Two-Person Control” or TPC	U		N/A	N/A	

Emergency Response Group Rally Points	U		N/A	N/A	
Northern Distribution Network (NDN)	U		N/A	N/A	References to network and/or routes only
Bilateral NDN Negotiations	C-S		1.4(a)	Date 25 years from creation date	Specifics of ongoing negotiations with NDN countries, i.e., Uzbekistan, Kazakhstan,
Movements supporting classified cargo in support of Foreign Military Sales (FMS)	S		1.4(a)	Date 25 years from creation date	Information on a specific country and/or FMS cargo
Movements supporting Foreign Military Sales (FMS) of unclassified cargo	U		N/A	N/A	
Vessel Activation Messages	S		1.4(a)	Date 10 years from signed date of message	
Foreign Entity Vetting (FEV) Working Group (WG) meeting announcements; e-mails	(U)		N/A	N/A	
Subject of FEV WG meetings	U-TS			Classified subjects are declassified based on declassification from the source	FEV WG subject(s) are unclassified unless derived from classified information
FEV WG Recommendations	U-TS			Classified subjects are declassified based on declassification from the source	Recommendations based on classified derived information are classified at the same level as the source

USTRANSCOM FEV intelligence process and capabilities	S-TS		1.4(c)	Date 25 years from creation	
Capabilities at COOP sites	S		1.4(a)	Date 25 years from creation n	

Movement Data Base Elements (See note below table)	U//FOUO	AT21; Trans Viz; JFAST; AMP; SMS; IGC; CAMPS	N/A	N/A	These data elements singularly or when compiled together are UNCLASSIFIED //FOR OFFICIAL USE ONLY and approved for cross-domain transfer by manual or automated means from SIPRNet to NIPRNet to support command mission requirements (please only use approved means for cross transfer)

Movement Data Base Elements include: System Requirement Identifiers (e.g. TTAN for JOPES, SAAM ID for SRS, UUIDs); Requirement Owner Organization; Requirement Route (i.e. onload & offload locations, dates, times); System Transaction Data; ULN; UIC; UTC; Service Codes; Load POCs; Mission routing from origination to termination; Mission number; Scheduled and actual data (departure and arrival locations and times); Total STONs bulk, oversize, outsize; Total MTONs; Total square feet; TCN; Number of pieces; Cargo Length, width, and height; Cargo category codes; HAZMAT; personnel requiring transportation; Personnel manifest details; Cargo manifest details.

Attachment 6

SECURITY (INFORMATION, PERSONNEL, INDUSTRIAL AND PHYSICAL) AND ANTITERRORISM (TCJ3-M) CLASSIFICATION MATRIX

Information To Be Protected	Classification	Related System, Plan, Program or Project	Reason	Declassify On	Remarks
Physical security plan for USTRANSCOM facilities	U		N/A	N/A	N/A
Security incident Inquiry Officer investigation report	U		N/A	N/A	If report included derived classified Information, classification and declassification date is based on level of derived information
Safe combinations	U – TS		1.4(g)	Date the combination changes	Classification of combinations depends on highest classification of information stored in the safe
Mission degradation based on a terrorist attack on USTRANSCOM facilities, personnel, mission critical assets	S		1.4(g)	Date 10 years from the date of attack	N/A
General Information on a Terrorist attack at Scott AFB against USTRANSCOM facilities, personnel,	U		N/A	N/A	N/A

mission critical assets					
USTRANSCOM mission critical assets listed by priority	S		1.4(g)	Date 25 years from date of identification of asset	N/A
Vulnerabilities of USTRANSCOM mission critical assets	S		1.4(g)	Date 25 years from date of identification of the vulnerability	N/A
Gaps in the protection of USTRANSCOM mission critical assets	S		1.4 (g)	Date 25 years from date of identification of the protection gap	N/A
Security aspects of USTRANSCOM alternate command sites	S			Date no longer than 25 years from date of original classification	N/A
Criticality assessment of USTRANSCOM mission critical assets	S		1.4(g)	Date no longer than 25 years from date of original classification	N/A
Loss or failure of electronic security systems for one or more USTRANSCOM facilities	U		N/A	N/A	N/A
Loss of classified materials	C		1.4(g)	Date one year from date of loss	N/A
Vulnerabilities recorded in local annual vulnerability	S		1.4(g)	Date 25 years from date of vulnerability assessment	N/A

assessments of USTRANSCOM buildings on Scott AFB					
Vulnerabilities recorded in local annual vulnerability assessments of USTRANSCOM Courier Stations	S		1.4(g)	Date 25 years from date of VA	N/A
Duress Codes	U//FOUO		N/A	N/A	N/A
USTRANSCOM directed security Stand Down Day training	U		N/A	N/A	Classified portions are derivative, not USTRANSCOM originally classified
Security measures for USTRANSCOM Commander while on Scott AFB during FPCON level A-B	U//FOUO		N/A	N/A	Security measures are U//FOUO per FOIA exemption 7
Security measures for USTRANSCOM Commander while on Scott AFB during FPCON levels C-D	S		1.4(a)	Date 30 days after lowering of FPCON from level C to A or B	N/A
Security measures for USTRANSCOM Commander during travel	U//FOUO		N/A	N/A	Security measures are U//FOUO per FOIA exemption 7
Vulnerabilities pertaining to the network and listed in CMI checklist by Cyber Operations Center	S		1.4(g)	Date 10 years from the date of the CMI checklist	CMI checklists involving spillages of classified information on the NIPRNet are not classified

					unless a network vulnerability is listed
Insider threats to USTRANSCOM personnel, buildings, systems	U		N/A	N/A	N/A
Information pertaining to potential violence in USTRANSCOM buildings by a USTRANSCOM employee or a person not a member of USTRANSCOM	U//FOUO		N/A	N/A	FOUO dissemination control marking authorized per FOIA exemption 7

Attachment 7

INFORMATION OPERATIONS (TCJ3-MI) CLASSIFICATION MATRIX

Information To Be Protected	Classification	Related System, Plan, Program or Project	Reason	Declassify On	Remarks
Operational Security (OPSEC) vulnerabilities	S		1.4(g)	Date 10 years from date of identification	
Operational Security (OPSEC) plans	C – S		1.4(g)	Date 10 years from creation of plan	
Operational Security capabilities and practices	S		1.4(g)	Date 10 years from date of identification	
Deception planning, operations, or estimates of effectiveness	S – TS		1.4(a), 1.4(b), 1.4(c), 1.4(g)	Date 10 years from date of identification	
Specific methods, technology, plans to counter network attacks	S – TS		1.4(a), 1.4(b), 1.4(c), 1.4(g)	Date 10 years from date of identification	
Current Information Condition (INFOCON)	U		N/A	N/A	
Espionage or other insider threats within USTRANSCOM	S – TS		1.4(a), 1.4(b), 1.4(c), 1.4(g)	Date 25 years	

Attachment 8

STRATEGY, POLICY, AND LOGISTICS (TCJ5/J4) CLASSIFICATION MATRIX

Information To Be Protected	Classification	Related System, Plan, Program or Project	Reason	Declassify On	Remarks
Integrated Priority List (IPL) submitted by USTRANSCOM	S		1.4(g)	10 years from the date of creation	Information revealing capability gaps/ vulnerabilities incorporated into the Comprehensive Joint Assessment (CJA)
Integrated Priority List (IPL) submitted by organization external to USTRANSCOM	U - TS		N/A	N/A	Derivative classification, marking must be carried forward.
Capabilities Joint Assessment (CJA)	S		1.4(e)	10 years from the date of creation	
Desire for agreements between countries	S		1.4(b)	Day of completion of negotiations and signed completion	
Status of negotiations of agreements between countries	S		1.4(b)	Day of completion of negotiations and signed completion	

Attachment 9

COMMAND, CONTROL, COMMUNICATIONS AND CYBER SYSTEMS (TCJ6)
CLASSIFICATION MATRIX

Information To Be Protected	Classification	Related System, Plan, Program or Project	Reason	Declassify On	Remarks
Vulnerabilities of USTRANSCOM systems/data located on SIPRNet	S		1.4(a), 1.4(g)	See DISA CIRCULAR 300-115-3.	Reference DISA CIRCULAR 300-115-3. Approval of concerned Program or Network Information Assurance Manager is required for distribution.
Vulnerabilities of USTRANSCOM NIPRNet	U//FOUO				Dissemination control marking of FOR OFFICIAL USE ONLY is applied. Approval of concerned Program or Network Information Assurance Manager is required for distribution.
COMSEC incidents or violations	C – TS			See NSTISSI 4003, Section VII, para 22	Incident reports are classified according to content (NSTISSI 4003, Section VII, para 22)
SIPRNet outages	C – S		1.4(g)	See DISA Circular 300-115-3, 1 June 2013	See DISA Circular 300-115-3, 1 June 2013, items 2.4.2.; 3.4.4.;

					3.4.5
NIPRNet Infrastructure downtime or outages	U//FOUO		N/A	N/A	Network down times will not be distributed outside USTRANSCOM. FOUO dissemination control marking authorized per FOIA exemption 2
Login for NIPRNet	U		N/A	N/A	
Passwords for SIPRNET	S		1.4(g)	Date 30 days after changing to new password	Passwords must be protected
Network attacks (phishing; hackers; probes)	S – TS		1.4(a)	Date 10 years from identification	
List of commercial companies with access to USTRANSCOM network	U//FOUO		N/A	N/A	FOUO dissemination control marking authorized per FOIA exemption 4
Capabilities of USTRANSCOM IT systems	U		N/A	N/A	
DRSN phone enabling codes	S-TS		1.4(g)	Date 90 days after changing to new codes	Codes are classified at level of enabled phone

Attachment 10

FINANCIAL INFORMATION OPERATIONS (TCJ8) CLASSIFICATION MATRIX

Information To Be Protected	Classification	Related System, Plan, Program or Project	Reason	Declassify On	Remarks
Transportation Working Capital Fund	U		N/A	N/A	
Government Purchase Card (GPC) purchases	U		N/A	N/A	

Attachment 11

ACQUISITION INFORMATION (TCAQ) CLASSIFICATION MATRIX

Information To Be Protected	Classification	Related System, Plan, Program or Project	Reason	Declassify On	Remarks
Contracts with requirements for contractor employees to access classified information	U		N/A	N/A	
List of commercial companies with contracts with USTRANSCOM	U		N/A	N/A	Do not disseminate without TCAQ approval
Contractual information identifying the contractor company	U		N/A	N/A	TCAQ coordination required before dissemination

Attachment 12

INSPECTOR GENERAL (TCIG) CLASSIFICATION MATRIX

Information To Be Protected	Classification	Related System, Plan, Program or Project	Reason	Declassify On	Remarks
USTRANSCOM IG reports not containing vulnerability information	U		N/A	N/A	IG reports may contain dissemination control of FOR OFFICIAL USE ONLY if they meet one or more of FOIA exemptions 2-9
Vulnerabilities to USTRANSCOM personnel or buildings reported to IG	S		1.4(g)	Date 25 years from identification of the vulnerability	

Attachment 13

PUBLIC AFFAIRS (TCPA) CLASSIFICATION MATRIX

Information To Be Protected	Classification	Related System, Plan, Program or Project	Reason	Declassify On	Remarks
Personally Identifiable Information (PII)	U		N/A	N/A	Disclosure of records to an individual from a system of records is prohibited except with the person' consent or as otherwise authorized by DoDI 5400.11.
Information pertaining to workplace violence; active shooter; or a terrorist event upon USTRANSCOM personnel on Scott AFB	U		N/A	N/A	No information dissemination to non-DoD media sources without TCPA approval.

Attachment 14

HISTORICAL INFORMATION (TCRC) CLASSIFICATION MATRIX

Information To Be Protected	Classification	Related System, Plan, Program or Project	Reason	Declassify On	Remarks
Annual historical report not containing vulnerabilities of USTRANSCOM capabilities	U		N/A	N/A	
Vulnerabilities of USTRANSCOM capabilities listed in an annual historic report	S		1.4(g)	Date 25 years from date of report	

Attachment 15

SENIOR PERSONNEL TRAVEL/MEETINGS/CONFERENCES CLASSIFICATION MATRIX

Information To Be Protected	Classification	Related System, Plan, Program or Project	Reason	Declassify On	Remarks
USTRANSCOM OCONUS Commander travel itineraries containing the following combinations as shown in the below matrix:	See Matrix Below		1.4(g)	Date 30 days after completion of trip	Travel itineraries for other USTRANSCOM GO/FO/SES are not classified
Visiting Distinguished Visitors, arrival dates, times, locations, itinerary	U-C		1.4(g)	Date 30 days after completion of trip	
GO/FO/SES attendance at USTRANSCOM conferences on Scott AFB	U		N/A	N/A	

	UNCLASS	UNCLASS	UNCLASS	UNCLASS	UNCLASS	UNCLASS	UNCLASS	UNCLASS	UNCLASS	Secret	Secret	Secret	Secret	Secret	Secret	Secret
Date(s) of travel	X									X	X	X	X	X	X	X
Time(s) of departure		X											X		X	X
Time(s) of arrival			X											X	X	X
Flight number				X							X	X			X	X
Seat number					X							X			X	X
Hotel						X				X						X
Hotel Room Number							X			X						X
Arrival Location								X						X	X	X
Departure Location									X				X		X	X