U.S General Services Administration (GSA)

GSA Order: GSA Classified Courier Procedures
OMA 1025.1A
Office of Mission Assurance
omapolicy@gsa.gov

Purpose:

This Order outlines the proper procedures for preparing and transporting classified national security information.

Background:

GSA employees are responsible for safeguarding any classified materials in their possession. Practicing operations security will significantly limit any potential loss of information. Based on 32 CFR Parts 2001, Classified National Security Information, and Executive Order (E.O.) 13526, Classified National Security Information, GSA employees must follow the proper procedures for preparing and transporting classified national security information.

Applicability:

This Order applies to all GSA employees handling classified national security information.

Cancellation:

This Order supersedes GSA Order ADM 1025.1, Procedures for the U.S. General Services Administration Classified Couriers.

Summary of Changes:

This Order updates:

1. The format of the order to align with OAS 1832.1C, Internal Directives Management.
2. The name of the Order.
3. Terminology and procedures within the Order for consistency.
4. The Order to an OMA Order for consistency with ADM 5450.39D CHGE 1, GSA Delegations of Authority Manual, Chapter 17 Office of Mission Assurance.

5. **Appendix A: Sample Courier Card** to include additional language necessary if transporting materials via commercial transportation.

Signature:

/S/_____ 4/25/2025_____
Robert J. Carter Date
Associate Administrator
Office of Mission Assurance

Table of Contents

1. Procedures

Before a GSA classified courier can transport classified material, they must receive authorization in accordance with this Order. Authorization is completed by the issuance of a Courier Card by the OMA Chief Security Officer or designee. The classified courier receives the original card and a copy is maintained by GSA's Security Programs Branch. Security logs of GSA personnel authorized to transport classified material are maintained by the Security Programs Branch and include: employee's name, employee's SSN, what office the employee works from, classification level of material authorized to be transported, the Courier Card issuance date, and Courier Card expiration date.

Note: The Communications Security (COMSEC) Manager and Alternate COMSEC Manager are the only GSA employees authorized to approve the issuance, removal, and/or transport of COMSEC equipment.

1.1. Preparation of classified material (not to include classified IT equipment)

Classified information shall be transmitted and received in an authorized manner which ensures that evidence of tampering can be detected, that inadvertent access can be precluded, and that provides a method which assures timely delivery to the intended recipient.

1.1.1. Document transmittal receipt

A GSA document transmittal sheet must be completed prior to transporting any classified material from one location to the next. In the event a security incident occurs while in transit, such as when a package is lost, the document transmittal sheet will provide a record of the materials transported. The courier will complete the document transmittal receipt and provide a signed copy to the designated Site Security Manager (SSM), prior to packaging the classified document. The document transmittal receipt is unclassified and provides contact information for the sender and recipient, a summary of the classified material/equipment that is being transported (note: the summary cannot contain any classified information), and instructions for the recipient to provide receipt of the document once the document has been transported. The original document transmittal receipt is maintained by the SSM or COMSEC Manager, as appropriate, for tracking/record keeping purposes. A copy is placed inside the outer envelope, and, if

requested, a copy is made for the recipient and/or classified courier to keep for their own records.

1.1.2. Delivery to/from GSA (packaging)

Classified materials will be placed in two opaque envelopes prepared as follows:

1.1.2.1. Inner envelope

A classified courier shall do the following on the inner envelope:

- Attach the appropriate level cover sheet [Standard Form (SF) 703 – Top Secret; SF 704 – Secret; SF 705 – Confidential, or SCI cover sheet] to the face of the classified documents.
- Annotate the full address of the intended recipient, the full return address of the sender, the name of the intended recipient, and the sender.
- Prominently mark the envelope, front and back, top and bottom, with the highest classification of the material.
- Mark the envelope with a warning notice outlining any specific or necessary handling instructions for the particular document(s).
- Seal the envelope with reinforced tape of such strength and durability as to provide security protection, prevent items from breaking through the package, and permit detection or evidence of tampering.
- IT equipment (e.g., laptop computers) must be configured to ensure that classified information does not become visible during the booting up process.

1.1.2.2. Outer envelope

A classified courier shall do the following on the outer envelope:

- Place a copy of the document transmittal sheet inside the envelope.

- Place the sealed inner envelope inside the outer envelope. Annotate full address of the intended recipient and full address of the sender. Intended recipients shall only be included by names of an attention line.

- Seal the envelope with reinforced tape of such strength and durability as to provide security protection, prevent items from breaking through the package, and permit detection or evidence of tampering.

- For local transportation of classified materials, a locked briefcase or similar type of locking enclosure may serve as the outer envelope. The key must be removed from the briefcase during the transportation. The briefcase must have a nametag or other marking that denotes where the briefcase should be returned if found.

- Do not place any classification markings or additional warning notices on the outer envelope.

1.1.2.3. Removable media

A classified courier shall do the following on removable media:

- Ensure media is marked using an SF 706 - Top Secret label; SF 707 - Secret label; or SF 708 - Confidential label, as applicable.

- Media will be inserted into a protective case that offers protection from visual inspection should the outer container be opened.

- The protective case must be placed into a lockable container and locked.

- No classification markings should be on the exterior of the locking container. However, an address label that identifies an appropriate address to which the case

should be shipped in the event it is separated from the courier shall be attached.

1.1.2.4. Record keeping

An inventory of the classified materials being transported shall be recorded and maintained by the SSM and/or the GSA COMSEC Manager, as appropriate. Classified couriers may also keep a copy of the document transmittal receipt at their assigned duty station as a means for record keeping.

1.2. Classified IT systems

All classified IT equipment located inside GSA Sensitive Compartmented Information Facilities (SCIFs) is handled, serviced, safeguarded, and transported by an IT representative in accordance with the policies and procedures of the Defense Information Systems Agency. Approval must be obtained by the GSA COMSEC Manager or Alternate COMSEC Manager prior to removing any classified IT equipment from a GSA facility. The GSA COMSEC Manager receives a copy of all IT equipment transmittal receipts from the IT representative to ensure accountability of all classified IT systems located inside the SCIF.

1.3. In transit

The Courier Card, along with GSA identification, badge, or credentials must be immediately available for presentation upon request by an appropriate security or law enforcement authority.

To ensure all security requirements for transporting and storing the classified material have been met, couriers shall review all steps listed in Section 1.4. “Arrival” prior to transporting any classified material.

When transporting classified materials within the local area, the courier must proceed directly to the destination with no unnecessary convenience stops.

If a need arises to transport classified materials using commercial transportation (such as aircraft, bus, boat, ferry, etc.), prior written approval must be obtained from the OMA Chief Security Officer to ensure all other means for transmitting the information have been exhausted. Before approval is granted, the requester must provide sufficient justification as to why the materials must be hand-carried versus the use

of other approved means, such as U.S. Postal Service Registered Mail for Secret and Confidential materials. When transporting classified material via commercial transportation, specific language must be included on the Courier Card. If language referencing immunity from search or inspection was not included on the original Courier Card, an updated document must be requested and received prior to traveling via commercial transportation with classified material.

The materials being transported shall remain in the physical possession of the classified courier at all times. Classified material will not be left in hotel rooms, hotel safes, private residences, public lockers, unattended vehicles, etc.

If overnight stops are anticipated, arrangements must be made prior to departure to store the materials at the nearest approved storage facility (military installation, U.S. Government Federal Facility, or cleared contractor facility with approved storage authorization at the same level or higher than the materials being transported). In the event of unanticipated overnight stops, the classified courier must contact the nearest facility as identified above to arrange for proper storage.

When in-transit storage is used at an approved facility, the package(s) shall remain sealed and transmittal receipts will be used.

Packages will never be opened, read, displayed, or otherwise viewed in any manner in public conveyances or places.

Under no circumstances may a laptop computer containing classified information be placed in use while in transit with the following exception:

> When requested by a Transportation Security Administration (TSA) screening official, a classified courier may boot up a laptop computer provided that sufficient protection is provided to prevent unauthorized disclosure of classified information. IT equipment (e.g., laptop computers) must be configured to ensure that classified information does not become visible during the booting up process.

Packages shall not be stored in any detachable storage compartments such as automobile trailers, luggage racks, vehicle trunks, passenger compartments, aircraft travel pods, or drop tanks. Further, classified couriers cannot leave classified material in locked vehicles, car trunks,

commercial storage lockers, or storage compartments in the passenger section of commercial airlines, or while aboard trains or buses.

All classified material must be transported in carry-on luggage. Classified couriers cannot pack classified items in regular checked baggage. Unless special circumstances exist, the hand-carried materials will be subjected to x-ray screening. If necessary, the screening official may also be allowed to feel, flex, and weigh the package without opening the envelopes themselves. The person screening the package will not, under any circumstances, be allowed to open the package. If an attempt to open the package occurs, the courier shall request an airport security supervisor. If the situation cannot be remedied without the package being opened, the courier shall contact the OMA Chief Security Officer or designee cited on the Courier Authorization Card or Letter before proceeding. Again, do not permit the screening official to open envelopes or read any portion of the classified document as a condition for boarding.

The classified courier must not discuss classified information in public or discuss the fact that they are hand-carrying classified material.

1.4. Arrival

Upon arrival at the destination, the classified courier must proceed directly to the approved facility to deliver or store the material. The classified courier must ensure that appropriate storage is available at the point of destination (e.g., GSA-approved security containers for collateral classified materials; approved facilities for SCI). The classified courier shall not leave classified packages in unattended offices.

The classified courier must verify with GSA's Personnel Security Division that the recipient has an appropriate security clearance and a need-to-know. The classified courier shall not leave classified material with any person other than the intended recipient unless that individual's security clearance and authority to act as the recipient's agent is verified. See GSA Order OMA 1000.2A, GSA Clearance Verification-Passing Procedures for further details.

The classified courier must inform the intended recipient of the classification level of the materials and any additional security requirements.

The classified courier must ensure transmittal receipts are prepared, signed, and are transmitted to the SSM.

1.5. Sanctions

Any person who suspects or has knowledge of a violation, including the known or suspected loss or compromise of Classified National Security Information, shall promptly report the violation to the individual's local GSA SSM and the OMA Chief Security Officer.

1.5.1. Violations subject to sanctions

Personnel shall be subject to appropriate sanctions if they:

- Knowingly, willfully, or negligently disclose to unauthorized persons information classified under E.O. 13526, Classified National Security Information, or any of its predecessor Orders.
- Knowingly, willfully, or negligently violate any other provisions of E.O. 13526, or any of its predecessor Orders, or knowingly and willfully grant eligibility for, or allow access to, classified information in violation of E.O. 13526, or any of its predecessor Orders or implementing directives.

Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation. Sanctions may be imposed upon any person who, regardless of office or level of employment, is responsible for a violation specified under this section as determined appropriate.

2. Definitions

2.1. Classified courier

A GSA employee identified by the OMA Chief Security Officer or designee as being authorized to transport classified materials.

2.2. Classified national security information or classified information

Information that has been determined pursuant to E.O. 13526 or any of its predecessor Orders to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. For purposes of this GSA Order, the term “classified material” is used interchangeably with the term “classified information.”

2.3. Classification level

This is the classification assignment that indicates the relative importance of classified information to national security, and thereby determines the specific security requirements applicable to that information. The three levels of classification of material to be transported are Confidential, Secret, and Top Secret.

2.4. Communications security (COMSEC)

This is the discipline of preventing unauthorized interceptors from accessing telecommunications in an intelligible form, while still delivering content to the intended recipients. Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications.

2.5. COMSEC equipment

Equipment designed to provide security to telecommunications by converting information to a form unintelligible to an unauthorized interceptor and, subsequently, by reconverting such information to its original form for authorized recipients; also, equipment designed specifically to aid in, or as an essential element of, the conversion process. COMSEC equipment includes crypto-equipment, crypto-ancillary equipment and authentication equipment.

2.6. COMSEC Manager

An individual designated by proper authority to be responsible for the receipt, transfer, accountability, safeguarding, and destruction of COMSEC material assigned to a COMSEC account.

2.7. Courier Card

Document authorizing a courier to transport classified material, issued by the OMA Personnel Security Branch per this Order.

2.8. Alternate COMSEC Manager

An individual designated in writing by proper authority to perform the duties of the COMSEC Manager during the temporary absence of the COMSEC Manager.

2.9. Need-to-know

A determination, after making any inquiries deemed necessary, that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized Governmental function.

2.10. Site security manager (SSM)

An individual assigned responsibility for the day-to-day security administration of classified programs and activities within a particular facility. SSMs must be appointed in writing.

3. Authorities

E.O. 13526 and 32 CFR Parts 2001.

4. Appendix A: Sample Courier Card

Appendix A: Sample Courier Card

Issuance Date: MM/DD/YYYY

To Whom It May Concern:

[NAME], [xxx-xx-xxxx], is an Official Courier for the United States of America, [Title/Division/Location]. ex: *Project Executive/Office of Design and Construction/Public Building Service/National Capital Region U.S. General Services Administration 1800 F Streets, NW, Washington, DC 20405.*

This is an official Courier Card authorizing the above named individual to act as a courier to transport classified national security information and equipment at [level the individual is cleared will be inserted here] while on official U.S. Government business. In many instances, this individual will be removing classified material without obtaining a property pass.

The material is **NOT** subject to search or inspections.

The Federal Government, requiring protection from unauthorized viewing or inspection, hereby places you on notice that this is a classified shipment. Accordingly, this shipment is immune from search or inspection by any unauthorized persons, including State and Local authorities. In the event this individual is incapable of completing [his/her] mission, (whether by accident, injury, detention, or any other reason) please immediately notify the nearest GSA, Federal Bureau of Investigation, and/or United States Military installation office.

Courier Card Expiration: MM/DD/YYYY

_____

[Name]
[Title (OMA Chief Security Officer or designee)]
Office of Mission Assurance
General Services Administration