U.S. General Services Administration (GSA)

GSA Order: GSA Clearance Verification-Passing Procedures
OMA 1000.2A
Office of Mission Assurance
omapolicy@gsa.gov

Purpose:

This Order outlines procedures for U.S. General Services Administration (GSA) personnel to verify an individual has the appropriate clearance level prior to sharing classified information and provides the procedures to follow when requesting to have clearance information passed to another agency or company.

Background:

GSA employees and contractor employees must ensure an individual has the proper clearance, access level and a need-to-know prior to sharing classified information. Need-to-know is the determination made by an authorized holder of classified information that access to the information is required by another appropriately cleared individual in order to perform official duties. Having a security clearance does not give automatic approval for access to classified information. The procedures in this Order outline the processes that will confirm if an individual has the appropriate clearance level for the purpose of sharing classified information.

When an external party wants to share classified information with a GSA employee or contractor employee, they also need to verify that the GSA employee/contractor employee has a valid clearance, which may include Sensitive Compartmented Information (SCI) access(es). This is accomplished by the GSA Personnel Security Branch passing clearance information (i.e., verifying to an external party that the GSA employee/contractor employee has the appropriate clearance and/or SCI access). The procedures in this Order outline the processes that are required to request GSA pass clearance or SCI access.

Applicability:

This Order applies to all GSA employees and contractor employees in the performance of their duties, except for the employees in the following independent offices within GSA:

1. The Office of Inspector General.
2. The Civilian Board of Contract Appeals.

Cancellation:

This Order supersedes OMA 1000.2, GSA Clearance Verification-Passing Procedures.

Summary of Changes:

This Order updates:

1. The contact information for submitting requests.
2. The submission time for requests is 2 business days across all documents and requests.
3. The format of the order to align with OAS 1832.1C, Internal Directives Management.

Signature:

/S/_____ 5/22/24_____
ROBERT J. CARTER Date
Associate Administrator
Office of Mission Assurance

Table of Contents

Table of Contents **3**
1. Internal GSA Clearance Verification **4**
1.1 Collateral Clearance Verification Submission 4
1.2 Sensitive Compartmented Information (SCI) Access Verification Submission 4
2. External Clearance Verification to GSA **4**
2.1 What is a Visit Authorization Request (VAR)? 4
2.2 Visit Authorization Request Steps 5
2.3 Collateral Clearance VAR Submission 5
2.4 SCI Access VAR Submission 6
3. Passing Clearance Verification Outside GSA **6**
4. Appendix A: GSA 6102, Passing Visit Authorization Letter Request **6**

1. Internal GSA Clearance Verification

To verify the clearance level of a GSA employee or contractor employee for another GSA employee or contractor employee, requests must be submitted at least two business days in advance of needing the clearance verified. After your verification request is received, you should receive a response within one business day. If you have not received a response within one business day, follow up on your request via email. Under no circumstances can classified information be shared without clearance verification.

What must an internal GSA clearance verification request include?

1. Full name, title, and office of the individual requesting the clearance verification.
2. Classification level of information you seek to share.
3. Purpose of sharing the information. Note: this description must be unclassified.
4. Full name, title, and office of the individual(s) for whom security clearance is to be verified.

1.1 Collateral Clearance Verification Submission

For confidential, secret or top secret clearance verification, submit your request to the GSA Personnel Security Branch at gsa.securityoffice@gsa.gov.

1.2 Sensitive Compartmented Information (SCI) Access Verification Submission

To verify if a GSA employee or contractor employee is briefed into specific SCI Access, submit your request to the Security Programs Branch (SPB) at SecurityPrograms@gsa.gov.

2. External Clearance Verification to GSA

GSA employees and contractor employees must verify the clearance or access level of an individual prior to sharing classified information with someone who is external to GSA (i.e., not a GSA employee or contractor employee) via receipt of a Visit Authorization Request (VAR).

2.1 What is a Visit Authorization Request (VAR)?

A VAR is how an external entity requests permission for a GSA employee or contractor employee to share classified information with an employee of the external entity. The VAR must include the following items:

1. Full name, title, email address, and agency or office of the individual whose clearance is being verified.
2. Clearance level held by the individual in question, investigation type and date, and contact information for the verifying official or office passing the clearance verification to GSA.
3. Purpose of visit or need for said information. Note: this description must be unclassified.
4. Date(s) of intended visit or meeting.
5. Name and email address of the GSA Point of Contact (POC) for the visit.
6. This information should be provided via one of the following methods:
    - A letter on company or agency letterhead.
    - An official form internal to requestor's agency.

2.2 Visit Authorization Request Steps

1. Notify the GSA Personnel Security Branch or GSA SPB, as specified below, that you are the GSA POC for an upcoming visit and from whom they should expect a VAR.
2. Notify the individual you would like to share classified information with (the requestor) that they must have their Agency or company send a password-protected VAR in an unclassified email or via fax, as specified below, at least two business days before their visit or planned meeting to discuss classified information.
3. A verification email should be sent to both the requestor and the GSA POC within one business day of receipt of the VAR. If you or the requestor have not received the email verification within one business day, send an email to check on the status of the email listed by the level of clearance you are verifying.
4. The GSA POC should share the verification email with other GSA employees or contractor employees who will be participating in the visit.

2.3 Collateral Clearance VAR Submission

For confidential, secret or top secret clearance verification, individuals should submit their VAR to the GSA Personnel Security Branch at gsa.securityoffice@gsa.gov or fax at (202) 219-0572.

2.4 SCI Access VAR Submission

The VAR needs to also include the SCI brief date if SCI Access is needed.

For SCI access verification, notify the individual their request should be submitted to the SPB at SecurityPrograms@gsa.gov or fax at (202) 219-3254.

3. Passing Clearance Verification Outside GSA

All GSA employee requests to pass a collateral clearance and/or any SCI access to a non-GSA entity must be submitted on a completed copy of **Appendix A: GSA 6102, *Passing Visit Authorization Letter Request*** at least two business days in advance. If you have not received a response within one business day, contact the office you submitted your request to in order to check on the status. To pass a confidential, secret or top secret clearance, completed forms should be submitted to the GSA Personnel Security Branch at gsa.securityoffice@gsa.gov or or fax at (202) 219-0572. To pass SCI access, completed forms should be submitted to the SPB at SecurityPrograms@gsa.gov or fax at (202) 219-3254.

GSA contractor employees must contact the Facility Security Officer at their contract company to request to pass their confidential, secret, top secret clearance, orSCI access verification.

4. Appendix A: GSA 6102, Passing Visit Authorization Letter Request