

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)

## A

The ability and opportunity to obtain knowledge of classified information.

[Back to Top](#)

## B

### Authorized Person

A person (recipient) who has a favorable determination of eligibility for access to classified information, has signed a SF 312, and has a need to know for the specific classified information in the performance of official

[Back to Top](#)

### CFR

Code of Federal Regulations

### CI

Counterintelligence

### Classified Data Spill

Commonly referred to as a “spill.” The accidental or intentional disclosure of classified information across computer systems. See also Negligent Discharge of Classified Information (NDCI).

### Classified Information

Information that has been determined pursuant to EO 13526, or any successor order, EO 12951, or any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011), to require protection against unauthorized

### Classifier

An individual who makes a classification determination and applies a security classification to information or material. A classifier may be an OCA or a person who derivatively assigns a security classification based on a properly classified source or a classification guide.

### Cleared Contractor

A person or facility operating under the National Industrial Security Program (NISP) that has had an administrative determination that they are eligible, from a security point of view, for access to classified information of a certain level (and all lower levels). There are approximately 8,500 cleared contractors with over

### Cleared Employee

A person who has been granted access to classified information, other than the President and Vice President, employed by, or detailed or assigned to, a department or agency, including members of the Armed Forces; an expert or consultant to a department or agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of a department or agency including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of a

C	
	department or agency as determined by the appropriate department or agency head.
<b>Compromise</b>	An unauthorized disclosure of classified information.
<b>CUI</b>	Controlled Unclassified Information

[Back to Top](#)

D	
<b>Damage Assessment</b>	A formal multi-disciplinary analysis to determine the effect of a compromise of classified information on the national security.
<b>Damage to the National Security</b>	Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.
<b>Declassification</b>	The authorized change in the status of information from classified information to unclassified information.
<b>Departments and Agencies</b>	Refers to any “Executive agency,” as defined in 5 U.S.C. 105; any “Military department,” as defined in 5 U.S.C. 102; any “independent establishment,” as defined in 5 U.S.C. 104; and any other entity within the executive branch that comes into the possession of classified information.
<b>Derivative Classification</b>	Incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.
<b>DoD</b>	Department of Defense
<b>DoDD</b>	Department of Defense Directive
<b>DoDI</b>	Department of Defense Instruction
<b>DoDM</b>	Department of Defense Manual
<b>DOPSR</b>	Defense Office of Prepublication and Security Review
<b>Downgrading</b>	A determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

[Back to Top](#)

E	
<b>ELO</b>	Enabling Learning Objective
<b>Employee</b>	For purposes of the National Insider Threat Policy, “employee” has the meaning provided in section 1.1(e) of EO 12968; specifically: a person, other than the President and Vice President, employed by, detailed or assigned to, a department or agency, including members of the Armed Forces; an expert or consultant to a department or agency; an industrial or commercial contractor, licensee,

<b>E</b>	
	certificate holder, or grantee of a department or agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of a department or agency as determined by the appropriate department or agency head.
<b>EO</b>	Executive Order
<b>Espionage</b>	Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.

[Back to Top](#)

<b>F</b>	

[Back to Top](#)

<b>G</b>	
<b>Government Contracting Activity</b>	An element of an agency designated by the agency head and delegated broad authority regarding acquisition functions.

[Back to Top](#)

<b>H</b>	

[Back to Top](#)

<b>I</b>	
<b>ICD</b>	Intelligence Community Directive
<b>ISSM</b>	Information System Security Manager (formerly Information Assurance Manager). The individual responsible for the cybersecurity (formerly information assurance) program of a DoD information system or organization.
<b>Inquiry</b>	The initial fact-finding and analysis process to determine the facts of any security incident.
<b>Insider</b>	Any person with authorized access to any United States Government resource to include personnel, facilities, information, equipment, networks or systems.
<b>Insider Threat</b>	The threat that an insider will use their authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.
<b>Investigation</b>	An in-depth, comprehensive examination of the facts associated with a security violation.

[Back to Top](#)

J

[Back to Top](#)

K

[Back to Top](#)

L

<b>Leak</b>	Deliberate disclosure of classified information to the public media.
-------------	--

[Back to Top](#)

M

[Back to Top](#)

N

<b>National Security</b>	A collective term encompassing both national defense and foreign relations of the United States.
<b>NDA</b>	Nondisclosure Agreement
<b>NDCI</b>	Negligent Discharge of Classified Information. A negligent spillage or unauthorized disclosure of classified information. Also see Classified Data Spill.
<b>Need to Know</b>	A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.
<b>NISPOM</b>	National Industrial Security Program Operating Manual

[Back to Top](#)

O

<b>OCA</b>	Original Classification Authority. An individual authorized in writing, either by the President, the Vice President, or by agency heads or other officials designated by the President, to originally classify information.
------------	---

[Back to Top](#)

P

<b>PAO</b>	Public Affairs Office
<b>Public Media</b>	A medium of communications designed to reach the public. Public media includes print media (e.g., newspapers, magazines, books), broadcast media (e.g., radio, television) and Internet media (e.g., websites, blogs, tweets).

[Back to Top](#)

Q

[Back to Top](#)

R

[Back to Top](#)

**SAP**

Special Access Program. A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

**Security Clearance**

A determination that a person is eligible for access to classified information.

[Back to Top](#)

T

Terminal Learning Objective

[Back to Top](#)

U

**Unauthorized Disclosure (UD)**

A communication or physical transfer of classified information to an unauthorized recipient.

[Back to Top](#)

V

Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information.

[Back to Top](#)

W

**WPEA**

Whistleblower Protection Enhancement Act

[Back to Top](#)

X

[Back to Top](#)

Y

[Back to Top](#)

Z

[Back to Top](#)