Office of the United States Trade Representative

Executive Office of the President

CLASSIFICATION GUIDANCE

Issued: April 2018
approved by: Jamieson Greer, Chief of Staff
point of contact: Stacey Williams, Director, USTR Office of Security

PURPOSE

To provide authoritative classification guidance and establish the Office of the United States Trade Representative (USTR) policies and procedures for classifying, downgrading, and declassifying national security information. The Classification Guidance (Guidance) provides for the protection of USTR information and its availability to authorized users. All employees have a responsibility to ensure the information we work with every day is properly classified, marked, and safeguarded. This Guidance addresses information classified at the CONFIDENTIAL level, which comprises almost all of the classified national security information (CNSI) handled by USTR staff. Certain USTR staff with appropriate clearances may handle CNSI at the SECRET or TOP SECRET levels. For guidance on marking and handling SECRET or TOP SECRET CNSI, contact the USTR Office of Security, which is part of the USTR Office of Administration.

AUTHORITY FOR THE GUIDANCE

Executive Order 13526, *Classified National Security Information* (Order) and 32 C.F.R. Part 2001, the Information Security Oversight Office (ISOO) implementing rules.

The USTR Office of Security is responsible for management of the USTR CNSI program. Direct questions about the USTR program to Stacey Williams, the Director of the USTR Office of Security.

CLASSIFICATION MANAGEMENT

Security clearance.

As part of the hiring processing, all USTR employees must apply for and be granted a security clearance at the 'SECRET' level or higher. When an interim or full security clearance is issued to an employee, s/he must attend an information security briefing and sign a non-disclosure agreement as a condition of the clearance.

Original and derivative classification authorities.

There are two types of classification authorities: original and derivative. Personnel not formally designated as an original classification authority (OCA) are, by definition, derivative classifiers.

Original classification authority (OCA). Original classification is the initial determination that disclosure of an item of information reasonably could be expected to cause damage to the national security. The Unites States Trade Representative limits OCA appointments to the minimum required for effective USTR operations and

delegates only to those USTR officials who have a demonstrable and continuing need to exercise OCA. The performance plans of each OCA includes the designation and management of classified information as a critical element.

Only the United States Trade Representative and those who hold positions to which s/he has delegated authority in writing may classify information originally. The OCA positions at USTR are listed in Attachment A.

Derivative classification authority. Derivative classification is the paraphrasing, restating, or generating in new form of information that already is classified, and marking the newly developed information consistent with the classification markings of the source of the information. Any USTR employee with an active security clearance may make a derivative classification decision.

Mandatory training.

All USTR employees who have been granted a security clearance must receive classification training. The USTR Office of Security is responsible for ensuring that OCAs receive initial and annual refresher training, and that all USTR employees who have an active security clearance receive derivative classification training at least once every two years.

Self-inspection program.

The Order requires every agency that originates or handles classified information to establish and maintain an ongoing self-inspection program designed to detect and eliminate or control conditions and practices that could result in the unauthorized or inadvertent disclosure of classified information. The USTR Office of Security carries out and reports on USTR's self-inspection program.

ELIGIBILITY FOR CLASSIFICATION

USTR cannot classify or maintain the classification of information in order to:

- Conceal violations of law, inefficiency, or administrative error
- Prevent embarrassment to a person, organization, or agency
- Restrain competition
- Prevent or delay the release of information that does not require protection in the interest of the national security

What are the criteria for classification?

USTR employees with original classification authority (OCAs) may consider information for classification only if ***all*** of the following criteria apply:

1. The U.S. Government owns, produces or controls the information;

2. The information has not been officially released or is not otherwise in the public domain;

3. The information pertains to one of the categories specified in the Order; **AND**

4. The OCA is able to identify or describe the damage unauthorized disclosure of the information reasonably could be expected to cause to national security.

What are the categories of information that USTR usually classifies?

For purposes of our work, the applicable categories of information that USTR typically classifies under the Order are:

- Foreign government information (FGI), which includes information the United States has provided to or received from a foreign government or international organization with the expectation that the information, the source of the information, or both, are to be held in confidence (Order section 1.4(b)).

    - *Example*: Information exchanged pursuant to a confidentiality arrangement with another country in the context of trade negotiations, such as the negotiating text, proposals of each government, accompanying explanatory material, and emails related to the substance of the negotiations.

- Foreign relations or foreign activities of the United States, including confidential sources (Order section 1.4(d)).

    - *Example*: Trade Policy Review Group (TPRG) or Trade Policy Staff Committee (TPSC) papers, instructions or interagency communications that reveal current or proposed U.S. government positions, discuss options in a trade negotiation or trade dispute, evaluate emerging policy challenges, or comment on the merits of current or anticipated foreign government positions.

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

    - *Example*: U.S. International Trade Commission (USITC) Probable Economic Effects Reports that include market overviews, background data that include probable economic effects advice, or reveal or can be used to derive USITC methodologies.

For guidance on handling SECRET and TOP SECRET CNSI, contact the USTR Office of Security, which is part of the USTR Office of Administration.

What is the correct classification level?

To determine the proper classification, the OCA must determine the level of damage to national security that could be expected from an unauthorized disclosure of the information. If unauthorized disclosure would cause:

- "Damage," the information should be classified as CONFIDENTIAL
- "Serious damage," the information should be classified as SECRET
- "Exceptionally grave damage," the information should be classified as TOP SECRET classification, which may be applied only by the United States Trade Representative

USTR typically classifies information at the CONFIDENTIAL level. FGI is classified at the CONFIDENTIAL level because its unauthorized disclosure is presumed to cause damage to the national security. For guidance on handling SECRET and TOP SECRET CNSI, contact the USTR Office of Security.

DECLASSIFICATION

Maintaining a security classification beyond its usefulness is costly and administratively burdensome. The Order requires an OCA to establish at the time of classification the period during which the information is to be protected.

How long does information remain classified?

Under the Order, information cannot remain classified indefinitely. The presumption of disclosure and release should be the primary consideration in the preparation and dissemination of CNSI. In general, an OCA will assign an automatic declassification date either on a date certain that occurs on or before the day 10 years after the date of classification, or when an event that reasonably could be expected to take place within 10 years of the classification date occurs. For example, three years after the date FTA negotiations end or the FTA goes into force, whichever is earlier.

If the information is too sensitive to allow declassification within the first 10 years, an OCA may establish a classification period up to 25 years after the date of classification.

If approved by the Interagency Security Classification Appeals Panel, the United States Trade Representative may exempt information from automatic declassification for a period longer than 25 years after the date of classification. To do so, release should clearly and demonstrably be expected to:

- Reveal information, including FGI, which would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States. For example, information that would give other

countries insights into the U.S. government's current trade negotiating strategies or priorities or reveal confidential methodologies the United States currently uses to calculate the probable economic effects of contemplated tariff and other trade concessions.

- Violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years.

Only the United States Trade Representative may reclassify information after declassification and release to the public based on a document-by-document determination that reclassification is required to prevent significant and demonstrable damage to the national security and the information may be reasonably recovered without bringing undue attention to the information.

INFORMATION SHARING AND DISSEMINATION

With the public.

You cannot publicly disclose CNSI. Unauthorized disclosure is a violation of the terms of your security clearance and can result in loss of clearance, termination of employment, and criminal penalties. You also may not disclose sensitive unclassified information that is legally privileged, business confidential, or non-public to persons outside the federal government without prior authorization from USTR's Office of Public and Media Affairs or the Office of General Counsel, as appropriate.

With U.S. government personnel and advisors.

If the individual has a valid security clearance. You may disclose CNSI to USTR staff, to other executive branch personnel, to Members of Congress and congressional staff, and to trade advisory committee members, if they both require access to the CNSI to carry out their duties or to advise USTR and have the necessary security clearance. It is your responsibility to verify, before disclosing CNSI, that the potential recipient has an appropriate security clearance and a need-to-know.

Newly hired USTR personnel. If the security clearance of a newly hired USTR employee has not been fully adjudicated but is in process, the individual may be granted access to material that is highly sensitive, legally privileged, business confidential, or classified as CONFIDENTIAL FGI, if access is necessary to carry out their duties and the employee executes a non-disclosure agreement. The non-disclosure agreement requires an employee to agree to protect this nonpublic information from unauthorized use or disclosure.

Individuals without clearances. In limited circumstances and with the prior approval of the relevant Assistant U.S. Trade Representative or the Office of General Counsel, you may disclose material classified as CONFIDENTIAL FGI to congressional staff, executive branch personnel, or private sector trade advisors who do not have a security clearance if disclosure both is necessary to obtain essential advice and the individual

executes a non-disclosure agreement before being given access to the CONFIDENTIAL FGI.

With foreign nationals.

You may not disclose CNSI to foreign nationals, including officials of foreign governments or international organizations, other than as may be permitted under a written arrangement or procedures agreed to between USTR and the pertinent government or organization. Disclosure usually would be limited to CONFIDENTIAL FGI.

MARKING AND HANDLING CLASSIFIED INFORMATION

Classification markings are the usual means of communicating the need to protect CNSI. You must affix classification and control markings uniformly and conspicuously to all material regardless of media or format to ensure that USTR has a standardized, visible indication of the sensitivity of the CNSI.

Foreign Government Information (FGI). Almost all of the CNSI handled at USTR is FGI that an OCA has classified at the CONFIDENTIAL level.

How do we protect FGI? We use a two-step process to protect FGI. First, the United States and the foreign country or international organization must execute a confidentiality arrangement that describes the information to be protected, the declassification date, and the handling instructions. Second, an OCA listed in Attachment A, must make a classification determination that lists the covered information, the declassification date, and the handling instructions. The determination also provides an example of the markings USTR staff must use to protect the CONFIDENTIAL FGI. This includes a cover sheet and email banner. Attachment B provides a sample classification determination.

What kind of information do we protect? In the context of trade negotiations, covered information would include the negotiating text, proposals of each government, accompanying explanatory material, and emails related to the substance of the negotiations.

How long do we protect it? We generally set the declassification date as a term of years after the entry into force of an agreement or, if no agreement enters into force, a term of years after the completion of the last round of negotiations, whichever is earlier. For trade agreements, the period of protection typically has been three or four years.

How do we handle CONFIDENTIAL FGI? The Order allows 'modified handling' for CONFIDENTIAL FGI, which may be less restrictive than the safeguarding standards applicable to other kinds of information classified at the CONFIDENTIAL level. Generally, modified handling permits making copies and transmitting CONFIDENTIAL FGI over unclassified e-mail or fax, discussing CONFIDENTIAL FGI over non-secured

phone lines, and storing electronic CONFIDENTIAL FGI on unclassified computer systems and hard copies of documents and copies downloaded on electronic media in a locked or otherwise secure cabinet, room, or building. **Always refer to the specific handling instructions described in the relevant USTR classification determination.**

How do we mark CONFIDENTIAL FGI? Documents should be marked as [insert name of agreement, e.g., NAFTA] CONFIDENTIAL, Modified Handling Authorized (C/FGI-MOD). You should use a cover sheet like the one in Attachment B. You also should use the following signature block on emails and similar electronic documents:

> This email contains [insert name of agreement, e.g., NAFTA] Foreign Government Information, classified CONFIDENTIAL, modified handling authorized (C/FGI-MOD). Per the classification authorization issued on [insert date], the contents must be handled in a manner to avoid unauthorized disclosure for [insert number of years] after the entry into force of an agreement or [insert number of years] after the completion of the last round of negotiations, whichever occurs first.

For guidance on marking and handling SECRET and TOP SECRET CNSI, contact the USTR Office of Security.

Attachment A

THE UNITED STATES TRADE REPRESENTATIVE
EXECUTIVE OFFICE OF THE PRESIDENT
WASHINGTON, D.C. 20508

FROM: AMBASSADOR ROBERT E. LIGHTHIZER August 29, 2017

SUBJECT: USTR Original Classification Authority (OCA)

ISSUE

Memorialize Delegation of Original Classification Authority (OCA) at the Office of the United States Trade Representative (USTR).

BACKGROUND

To protect classified information against unauthorized disclosure, USTR leadership must properly classify information in accordance with classification guidelines in Executive Order 13526 and ISOO Directive One.

ACTION

The following executives are designated USTR OCAs and delegated original classification authority at the Secret and Confidential levels. They shall appropriately familiarize themselves with the procedures in making original classification decisions. They are encouraged to consult with the USTR Office of Security in carrying out their duties.

Deputy U.S. Trade Representatives (2)
Deputy U.S. Trade Representative & Chief of Mission, Geneva
Chief of Staff
General Counsel
Chief Agricultural Negotiator
Chief Innovation and Intellectual Property Negotiator
Chief of Mission, Geneva
Assistant USTR for Administration

ATTACHMENT B

EXECUTIVE OFFICE OF THE PRESIDENT

OFFICE OF THE UNITED STATES TRADE REPRESENTATIVE

WASHINGTON DC 20508

CLASSIFICATION AUTHORIZATION FOR KORUS NEGOTIATING DOCUMENTS

AUTHORIZED BY: JAMIESON GREER, CHIEF OF STAFF

DATE: JANUARY 5, 2018

Executive Order 13526 of December 29, 2009, authorizes classification of certain types of information, including foreign government information (FGI), if its unauthorized disclosure reasonably could be expected to cause identifiable or describable damage to the national security. *See* Section 1.4(b). FGI includes (1) information provided to the United States by a foreign government with the expectation that the information and/or its source will be held in confidence; or (2) information produced by the United States pursuant to a joint agreement with a foreign government requiring that the information be held in confidence. *See* Section 6.1(s). The unauthorized disclosure of FGI is presumed to damage the national security. *See* Section 1.1(d).

The United States and Korea are entering into negotiations regarding the United States – Korea Free Trade Agreement (KORUS) and have agreed to hold documents exchanged in the course of these negotiations in confidence.

As an Original Classification Authority at the Office of the United States Trade Representative, I have determined that information exchanged in confidence in the context of the KORUS negotiations, such as the negotiating documents, proposals of each Government, accompanying explanatory material, and written communications related to the substance of the negotiations, is FGI as defined in Executive Order 13526, the disclosure of which will harm the national security of the United States. Accordingly, I hereby classify these materials as Confidential Foreign Government Information pursuant to section 1.4(b) of Executive Order 13526.

The documents should be marked as KORUS CONFIDENTIAL, Modified Handling Authorized (C/FGI-MOD). These documents will be declassified four years after the entry into force of the results of these negotiations or, if no results enter into force, four years after the completion of the last round of negotiations, whichever is earlier. The documents should cite this classification authorization as the basis for classification and contain a short description of the authorized modified handling. A sample of this marking is enclosed.

Emails and similar electronic documents that contain or reflect KORUS CONFIDENTIAL, Modified Handling Authorized (C/FGI-MOD), should include the following signature block:

> *This email contains KORUS Foreign Government Information, classified CONFIDENTIAL, modified handling authorized (C/FGI-MOD). Per the classification authorization issued on January 5, 2018, the contents must be handled in a manner to avoid unauthorized disclosure for four years after the entry into force of the results of these negotiations or four years after the completion of the last round of negotiations, whichever occurs first.*

Attachments:

Sample Cover Page for KORUS Confidential Information
Instructions for setting up a KORUS Confidential signature block

Instructions for NAFTA E-mail Signature in Outlook

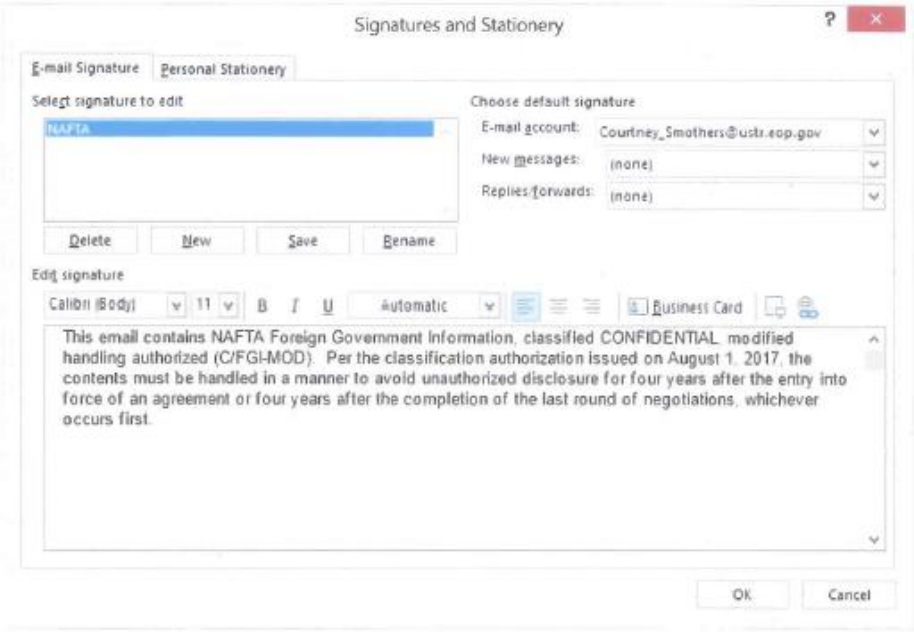
Each time you send an email related to the NAFTA negotiation, use a NAFTA signature block. Below are instructions for creating a NAFTA signature. You will need to select it for each email where you want it to appear.

1. Open Outlook and click on New to compose a new message, then click on the Insert tab on the Ribbon and Choose Signature.

2. Click on the New button on the Signatures and Stationery screen, type in a name for your signature, then click OK.

3. Create a title for your signature.

4. Now use the Edit signature box to compose your signature. The text below is the approved text for all NAFTA negotiation emails.



5. When you are done, click OK to proceed. Congratulations on your NAFTA signature!