

## Information Security Script

This briefing is being given by the Information Security Staff (ISS). The ISS is part of the Personnel and Document Security Division (PDSD). The other component of PDSD is the Personnel Security Branch (PSB), who processed your paperwork and adjudicated your background investigation to determine your eligibility for access to classified national security information. You have all had a favorable determination for access to classified information. You are required to receive annual security refresher training in order to maintain your security clearance.

There are two executive orders that USDA must adhere to working with classified information. The first is EO 12968, which tells us how we go about determining if someone is eligible for access to classified information. PSB is responsible for implementing this executive order. The second is EO 12958, as amended, which tells us once someone has been approved for access to classified information, how that person, and in essence everyone will treat classified information. ISS is responsible for implementing this executive order.

EO 12958 gives very specific categories that information must fall within to be eligible for classification. These categories include: military plans or weapons systems; foreign government information; intelligence activities; foreign relations or foreign activities; matters pertaining to national security including defense against transnational terrorism; nuclear materials; vulnerabilities or capabilities of systems, infrastructures, protection of national security, including defense against transnational terrorism; and weapons of mass destruction. Protection from transnational terrorism and weapons of mass destruction are new categories added post 9/11.

There are only three levels of classified information. They will always be color-coded, standard throughout the government. Orange for TS means it could cause *exceptionally grave damage*. Red for S means it could cause *serious damage*. And blue for C means it could cause *damage*.

Currently the Secretary of Agriculture is the only USDA individual who can originally classify a document. He is considered an Original Classification Authority or OCA. An OCA receives specific training on how to determine if information can or should be classified. You, on the other hand, can derivatively classify information.

When you derivatively classify something, you are extracting classified information from one document and incorporating it into another document. You must list your source document. You must also treat your derivative document in the same manner prescribed for your source document. Your source document should provide the declassification instructions. The ISS can provide you assistance with derivative classification.

Just about anything you can imagine can be classified. It is not just limited to paper products or telephone conversations. In some instances whole aircrafts and buildings are classified. Here are but a few examples of things that can be classified.

How will I know if something is classified? All classified material should be EXPLICITLY labeled. That means if it's a Secret document, then you should be able to look at it and determine automatically your looking at a Secret document. Classification markings should go at the top and bottom of the paper. Each paragraph, subject line, chart/graph, etc., should be marked. That is called portion marking. Cover sheets should be used when the document is not stored. As I mentioned previously, Confidential cover sheets are blue, Secret cover sheets are red, and Top Secret cover sheets are orange.

Here is an example of what a classified document should look like. You can see the overall classification level is at the top and bottom and the paragraphs are portion marked. The source document provides the date or event when the document can be declassified and where your classification is derived.

It's very important to point out that there are only three levels of classified information. You may be familiar with markings such as these. They are considered "Special Handling Markings" and not classification markings. This is information that is very sensitive, however, doesn't quite meet the requirements to be eligible for classification. For instance Department of State and Department of Defense use "Sensitive But Unclassified." The same is true for Law Enforcement Sensitive. USDA has created it's own caveat called Sensitive Security Information. The Secretary signed this regulation on January 30, 2003. The number is DM-3440-02, and can be found on the OCIO website under directives on USDA's website. The goal of the SSI caveat is to provide protection for that information that doesn't quite meet the requirements for one of the three levels of classification, yet is sensitive enough where protection from disclosure is necessary. Placing SSI on a document means the document should be reviewed and approved prior to releasing it to the public. In many cases, information would be removed before releasing the document.

A cover sheet was developed and is available through the USDA forms supply. Offices throughout USDA have been using these cover sheets for financial data, sensitive trade issues, informative memo's between management, and other types of information.

When we receive information from foreign government organizations and agencies, we are obliged to protect it, equal to the U.S. classifications. This means if you receive a foreign trade negotiation from Italy and they have it marked their equivalent to US Secret, we must protect their information as a classified "Secret" document. The new USDA DM 3440-001, Information Security Program Manual identifies each country and their classification markings.

There are procedures for safeguarding classified information, in every aspect of its life. We're going to cover them briefly here. If you would like more detailed information, you can contact either your agency security officer or the Information Security Staff. Our job is to help you.

Handcarrying classified between offices should be placed in an opaque envelope. If you need to take the information outside your building you must double-wrap the materials. That means using two opaque envelopes or placing the document in an envelope and a lockable courier bag. If you need information on purchasing a courier bag, you can either contact your agency security officer or the Information Security Staff.

When transporting classified materials out of USDA buildings, a current courier authorization letter is required. This letter is issued by Personnel and Document Security Division. The letter specifies the level of classified information you are authorized to transport, your security clearance level, and an expiration date. . You must always keep a copy of the letter with you during transportation of classified information and a valid USDA identification badge. It is your responsibility to also ensure the receiving individual and agency have the authority to store that level of classified material and the individual has the appropriate security clearance.

Classified material up to the Secret level can be sent through U.S. Post Office. Top Secret material must either be hand-carried or sent through an approved courier such as the Defense Courier Service. There are 9 contracted overnight services, such as, FedEx or DHL who can be used for Secret and Confidential information. Secret can be mailed through the US Postal Service using Registered Mail. Confidential can be sent Registered, Certified, or First Class Mail.

When sending Confidential information within the United States, the front of the envelope must be marked "Postmaster Do Not Forward - Return to Sender" . This requirement ensures that mail sent to individuals who have retired or changed jobs don't receive classified mail at a new job or residence.

All classification markings should be shown on the inner envelope. The intended recipient will also be listed on this envelope. It's imperative the envelope be taped up in a manner that someone attempted to open the envelope, it would be very apparent to anyone.

It's important to remember that on the outer envelope, no classification markings are to be shown. Also the package should be addressed to an activity approved to store classified at that level and place the person's name on the outer envelope. This has been a recent change. Previously you could not place a persons name on the outer envelope.

This is an actual package mailed through the U.S. postal system. Never mark packages in this way because it raises an automatic red flag. This was sent by an individual who worked in a very small office and was retiring.

When traveling, classified materials must be kept in their transport status at all times and under your constant surveillance. This means it cannot be opened and read in public. Classified material cannot be stored overnight in the trunk of a car, hotel room safe, or under your pillow. When necessary, alternate arrangements to store classified information in an approved security container can be made in advance, or when unexpected delays happen, call the USDA Emergency Operations Center at (202) 720-5711 for assistance. The Operations Center is open 24/7.

Taking classified information on a plane is not a preferred method. It's more efficient to send the information via US Postal Service or an overnight carrier. However, if it is necessary to board a plane with classified information you must remember to not stowe the information and keep it with you at all times. You must notify the airlines in advance and have a special courier letter prepared. Notify the ISS for additional preparations. Again, it's important to prepare for unusual delays in your travel itinerary.

Discussing or faxing classified information requires using encrypted equipment. This is necessary to protect the integrity of the information. This is an example of a secure telephone and secure fax. It takes both devices to send a classified fax. The phone can be used for classified discussions. The phone has a card inserted which holds the encryption key. When the card is removed the phone and the card are unclassified as long as they aren't stored together. Once they are together the device and the key are classified at the level the phone is approved for discussion. Some phones are only approved at the "Secret" level and others are approved for Top Secret. This applies to everyone!

As you can see, even the President is not exempt from using equipment specifically designated for classified usage. Here is President Bush, on September 11, 2001, at the elementary school. The room was secured and the STE was set up for the President to discuss the events. As he's talking the second plane is hitting the World Trade Center. This rule applies to everyone.

All classified processing must be done on a system that has been approved for classified usage. USDA OCIO is responsible for establishing policy on processing classified within USDA. You need to be aware that computers must be designated for classified processing and once a storage disk is placed in the system, the disk is then classified. Once a computer is used for classified processing, the computer must always be considered a classified piece of equipment. For more please contact the cyber security office in OCIO.

Copiers have multiple capabilities, such as, email, scan, and fax. Each capability creates a vulnerability for classified information. It's for this reason that machines are designated for classified processing. These machines have these capabilities disabled and they must be owned by USDA, as opposed to leasing. Copiers that have been used for classified reproduction must be excessed in a secure manner also. When you need to dispose of a copier that has been used to reproduce classified, contact the Information Security Staff for disposal procedures. If a classified copier isn't available to you, then you can always use the copy function on a CLASSIFIED fax machine. If no options are available to you, call the Information Security Staff for assistance in locating a copier you may use.

You can store Confidential and Secret in an office provided you have a GSA Security Container. Top Secret requires supplemental controls such as, an alarmed room with a 15 min response time or a 24/7 room occupation with TS cleared individuals. It's important to ensure your security container is a GSA security container. Using any other container is a security violation. The Information Security Staff can get information such as prices and sizes for purchasing a container.

These are examples of what type of lock you will find on an approved GSA security container. If your lock doesn't look like, there is a good chance your container isn't approved for classified storage. Another easy way to identify if your container is legal is a label that says it's a GSA Security container such as these. If your unsure, give the ISS a call and we'll be more than happy to look at your container and provide assistance to you.

NSA establishes the requirements for all destruction devices for classified information. USDA uses approved shredders or we burn the information using an agreement with the Pentagon. It's important to note that store bought shredders are not approved for classified information. If you don't have an NSA-approved destruction device and need to destroy some materials, contact the

Information Security Staff and we can assist you in locating the nearest approved shredder or make arrangements for the destruction of your classified materials.

Security infractions are administrative errors that never put the classified information at risk of possible compromise. An example of an infraction may be not signing an SF 702, Security Container Checksheet, when you open and close a security container. The information stored is not at risk, but that is an administrative requirement in place. A single infraction is not significant, but a pattern of many infractions can reveal a lack of appreciation or understanding of security procedures. It's for this reason that multiple infractions can be treated as a security violation.

A Security Violation is defined as any knowing, willing or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information. An example of this is taking classified information home to complete a project or using your office computer to process classified information. These definitely are actions considered a security violation.

Committing a security violation or multiple security violations can affect your security clearance. Here is the range of sanctions that can be applied to individuals and you can see it begins with a warning but can lead to criminal charges and loss of your job.

It's important to not that Espionage must involve an action or information that harms the US or give advantage to a foreign nation. This is not to be confused with Economic Espionage which is stealing trade secrets and primarily involves private industry.

Espionage is alive and well in the US. Even though it says there have been 150 individuals convicted of espionage, there have been hundreds of individuals suspected of espionage.

Let's look at some highly public cases of espionage. Of course you all know Bin Laden declared this was a holy war. His original declared motive was based on religious principles. He collected information against the government through open source information. Timothy McVeigh motive was anti-government. He hated the government and referred to Ruby Ridge and Waco as examples of his justification of hate. Robert Hanson was with the FBI for 27 years. He was a Russian spy for at least fifteen of those years and received over a million dollars in cash and diamonds for selling information. His espionage led to several agents being executed. In 2004, Larry Franklin, a DOD analyst working in the Pentagon, was passing classified information to an Israeli diplomat and a pro-Israel lobbying group "American Israel Public Affairs Committee" A search of his home revealed that he had 83 classified documents at his residence. His motives were political and he was a sympathizer. In Jan 06, he was sentenced to 12 years in prison for his espionage.

Regardless of the motive and ability to collect information for the purposes of sharing it with a foreign government to harm the US, you need to understand that your safety and our national security are one in the same. Everyone is responsible for the protection of our US information.