



# **CII/SSI Policy Guide**

**For**

**Employees, Vendors, Contractors or other  
Persons Accessing VDOT's CII/SSI**

An Accompanying Guide to CII/SSI Policy Version 6.0, March 2006 (Interim Revision – November, 2009)

**Interim Revision  
November, 2009**

# Table of Contents

I.	PURPOSE .....	3
II.	GUIDELINES FOR DESIGNATING AND MARKING VDOT INFORMATION AS CII/SSI.....	3
	Designating CII/SSI.....	3
	Marking CII/SSI.....	3
	Marking Maritime Related SSI.....	4
III.	GUIDELINES FOR HANDLING, STORING AND REPRODUCING CII/SSI.....	4
IV.	GUIDELINES FOR RELEASING DOCUMENTS DESIGNATED AS CII/SSI .....	4
V.	SAMPLE DOCUMENTS.....	5
	Frequently Asked Questions.....	6
	Quick Reference to Identifying CII/SSI.....	8
	CII/SSI Designation Decision Flowchart .....	9
	Multi-Purpose Non-Disclosure Agreement.....	10

**NOTE: The Multi-Purpose Non-Disclosure Agreement form included in this document is a sample form and should not be used as the actual form. The actual Multi-Purpose Non-Disclosure Agreement form may be downloaded from the *Inside VDOT* Forms page.**

# *CII/SSI Guide*

## **I. Purpose**

This Guide will provide general guidance the user/originator can use to designate CII/SSI in your sections and develop specific procedures for handling, marking, disseminating, releasing and destroying CII/SSI. You will also find samples of the forms that should be used in the aforementioned processes.

Critical infrastructure is a system or asset so vital that its incapacity or destruction would have a debilitating impact on security, economic security, public health or safety. ***Critical infrastructure information*** (CII) is the designation used by VDOT to identify information that is not appropriate for public release without a need-to-know. ***Sensitive security information*** (SSI) is the designation used to identify information related to **maritime** critical infrastructure that is not appropriate for public release without a need-to-know.

A page containing Frequently Asked Questions has been included in this Guide for your reference. If you have questions that are not answered in this guide, you may submit your questions to your contract manager. VDOT employees may submit questions via email, to [CriticalInfrastructure@VDOT.Virginia.gov](mailto:CriticalInfrastructure@VDOT.Virginia.gov) .

## **II. Guidelines for Designating and Marking VDOT Information as CII/SSI**

### **Designating CII/SSI**

Each Manager should perform a review of the documents in his/her custody to determine if the document contains CII/SSI and ensure proper markings are affixed. Additionally each vendor/contractor should review documents created in connection with the VDOT contract to ensure CII/SSI is properly marked and handled. This Guide contains a CII/SSI Designation Decision Process flowchart and Quick Reference document to provide you with the necessary tools in determining proper CII/SSI designation.

### **Marking CII/SSI**

Once a document has been designated as CII/SSI, it should be marked according to the following:

It is the responsibility of the document originator; VDOT employee or contractor/vendor to make sure that CII/SSI contained within the document is identified and marked, whether it has been previously marked or not. However, if you are the person handling a document which you feel contains CII/SSI and the document has not been properly marked; please refer the document back to the originator for designation and proper marking.

The marking shown below (frame and format optional) should be placed appropriately on all pages or sections containing CII material. It should be located either at the top or bottom of the page consistently throughout the document. The format and arrangement of the words may be modified to accommodate different situations but the wording should remain consistent. Appropriate font color needs to be utilized to ensure the markings are readily visible.

**– Restricted –  
Critical Infrastructure Information**

# *CII/SSI Guide*

## **Marking Maritime Related SSI**

Documents designated as SSI should be marked at the top of every page in the document and at the following locations in the document:

- The outside of any front cover,
- The outside of any back cover,
- Any binder cover or folder (front and back)
- Any title page

The marking at the top of the page should be:

**Sensitive Security Information**

The marking at the bottom of each page of the document should be:

**WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need-to-know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

## **III. Guidelines for Handling, Storing and Reproducing CII/SSI**

CII/SSI shall be protected at all times, either by appropriate storage or having it under the personal observation and control of a person authorized to receive it. Each person who works with protected CII/SSI is personally responsible for taking proper precautions to ensure that unauthorized persons do not gain access to it.

During working hours, reasonable steps shall be taken to minimize the risks of access to CII/SSI by unauthorized personnel. After working hours, CII/SSI shall be stored in a secure container, such as a locked desk, file cabinet or facility where contract security is provided.

CII/SSI shall be transmitted only by VDOT courier, US first class, express, certified or registered mail, or through secure electronic means.

CII/SSI in electronic format should be released in a protected format such as a locked PDF or password protected WORD document.

Material containing CII/SSI shall be disposed of by any method that prevents unauthorized retrieval and in accordance with established records retention policy.

Documents or materials containing CII/SSI may be reproduced to the minimum extent necessary to carry out official duties provided that the reproduced material is marked and protected in the same manner as the original material.

## **IV. Guidelines for releasing documents designated as CII/SSI**

Before CII/SSI can be released the following criteria need to be met;

- The requestor has a need-to-know the information,

## *CII/SSI Guide*

- The requestor has been cleared for access to CII/SSI material through VDOT's Criminal History Records Check process as required in DPM: 1-25,
- And the requestor completes and signs a Non Disclosure Agreement Form (NDA).

If the requestor does not have a need-to-know, refuses to sign the NDA form or does not meet the requirements outlined in DPM 1-25 do not release the information to them. If the requestor takes issue with this decision contact the contract manager if the request is contract related. For contract managers or if the request is not contract related please submit questions to

[CriticalInfrastructure@VDOT.Virginia.gov](mailto:CriticalInfrastructure@VDOT.Virginia.gov).

When non-disclosure agreements are completed for VDOT employees the signed non-disclosure agreements should be returned to the Human Resource Department to be filed in the employee's personnel folder. Contractor or Vendor NDA forms are to be maintained by the VDOT Contract Officer and should be filed with the procurement documents. When NDA forms are completed to release CII/SSI to a non employee, contractor or vendor the NDA form shall be maintained by the releasing custodian of the CII/SSI. A sample Non-disclosure agreement has been included for your reference.

### **V. Sample Documents**

This Guide contains the following Sample Forms:

- Frequently Asked Questions
- Quick Reference to Identifying CII/SSI
- Non-Disclosure Agreement
- CII/SSI Designation Decision Process flowchart

# *CII/SSI Guide*

## **Frequently Asked Questions**

### **1. What is CII?**

Critical infrastructure information (CII) is the designation used by VDOT to identify information that is not appropriate for public release without a need-to-know.

### **2. What is SSI?**

Sensitive security information (SSI) is the designation used to identify information related to **maritime** critical infrastructure that is not appropriate for public release without a need-to-know.

### **3. What is need-to-know?**

The legitimate requirement of a person or organization to know, access, or possess sensitive or classified information that is critical to the performance of an authorized, assigned mission (i.e. a VDOT related project). The necessity for access to, or knowledge or possession of, specific information required to carry out official duties. The information is intended for use only by individuals who require the information in the course of performing their job function.

### **4. What is Public Knowledge?**

Information about which knowledge or use is accessible to the general public if there has been no deliberate attempt to keep it hidden or secret. Knowledge that is available to anyone. Something might be considered public knowledge if it could be seen in a public area versus being located in a locked or non-public area. In some instances, the object itself may be public knowledge but it's location or use in that specific instance is not (e.g., an electrical panel in a reception area is recognizable and not hidden but, if the panel is locked, what the various circuit breakers control is not public knowledge).

For example, if a circuit breaker box is located in the lobby of a building, the location of that box would not be CII/SSI. However, the identification of the circuits/devices controlled by the breakers in the box might be CII/SS depending on the function of the devices controlled by the individual breakers (Security Systems, Alarm Systems, etc.). If the box is located in a locked room in an area not normally open to the public, it could be considered CII/SSI.

### **5. Who has to do the review and marking?**

It is the responsibility of the document creator to review the document for potential CII/SSI information and to mark the document accordingly. If a document recipient receives a document which contains CII/SSI information the recipient should forward the document back to the creator for proper marking.

### **6. Can A/E firms mark CII/SSI as the plans/specs are developed?**

The Contract Officer should inform the A/E firm at the time the contract is awarded that the project contains CII/SSI and the firm's responsibilities for marking information. As such, plans/specification must be marked accordingly as they are developed. A/E firms, or any other outside entity, who work as agents of VDOT must mark the CII/SSI in accordance with the Policy.

### **7. Can Vendors or Contractors release CII/SSI information to third parties?**

Vendors and Contractors can release CII/SSI to business partners or sub-contractors in connection with work performed under the terms of the contract only if a need-to-know has been established. The Vendor or Contractor will notify the VDOT Contract Officer who will ensure the Non Disclosure Agreement form is completed and the protocols outlined in DPM 1-25 are followed prior to the release of the CII/SSI.

### **8. What about solicitations that involve information and site-visits that contain/show CII/SSI?**

The current approach to handling CII/SSI in public advertisements:

- **Do not include CII/SSI in the public advertisement.**

The current approach to handling CII/SSI in pre-bid meetings:

- Require pre-registration for a mandatory pre-bid conference.
- Obtain signed non-disclosure agreements and verify identity with photo-id of all participants prior to allowing entry into the pre-bid meeting.

## *CII/SSI Guide*

- Sanitize CII/SSI material to work being solicited and to the extent needed to prepare a formal bid.
- Monitor pre-bid meeting and conduct site visits at the time of the pre-bid.
- Collect and account for all CII/SSI material after pre-bid meeting (no take away documents)
- Limit access and photography to that which is necessary to prepare a formal bid.

**Note: By following the guidance above, access to the CII/SSI material is “restricted” and therefore no Criminal History Records Check is required as indicated in DPM 1-25. If the guidance above is not followed, or if the extent of the project requires the contractors or vendors to leave the pre-bid meeting with the CII/SSI material then the access becomes “unrestricted” and a Criminal History Records Check is required as indicated in DPM 1-25.**

# CII/SSI Guide

## Quick Reference to Identifying CII/SSI

Information identified as either Critical Infrastructure Information or Sensitive Security Information (CII/SSI) should be marked as specified in the CII/SSI Policy.

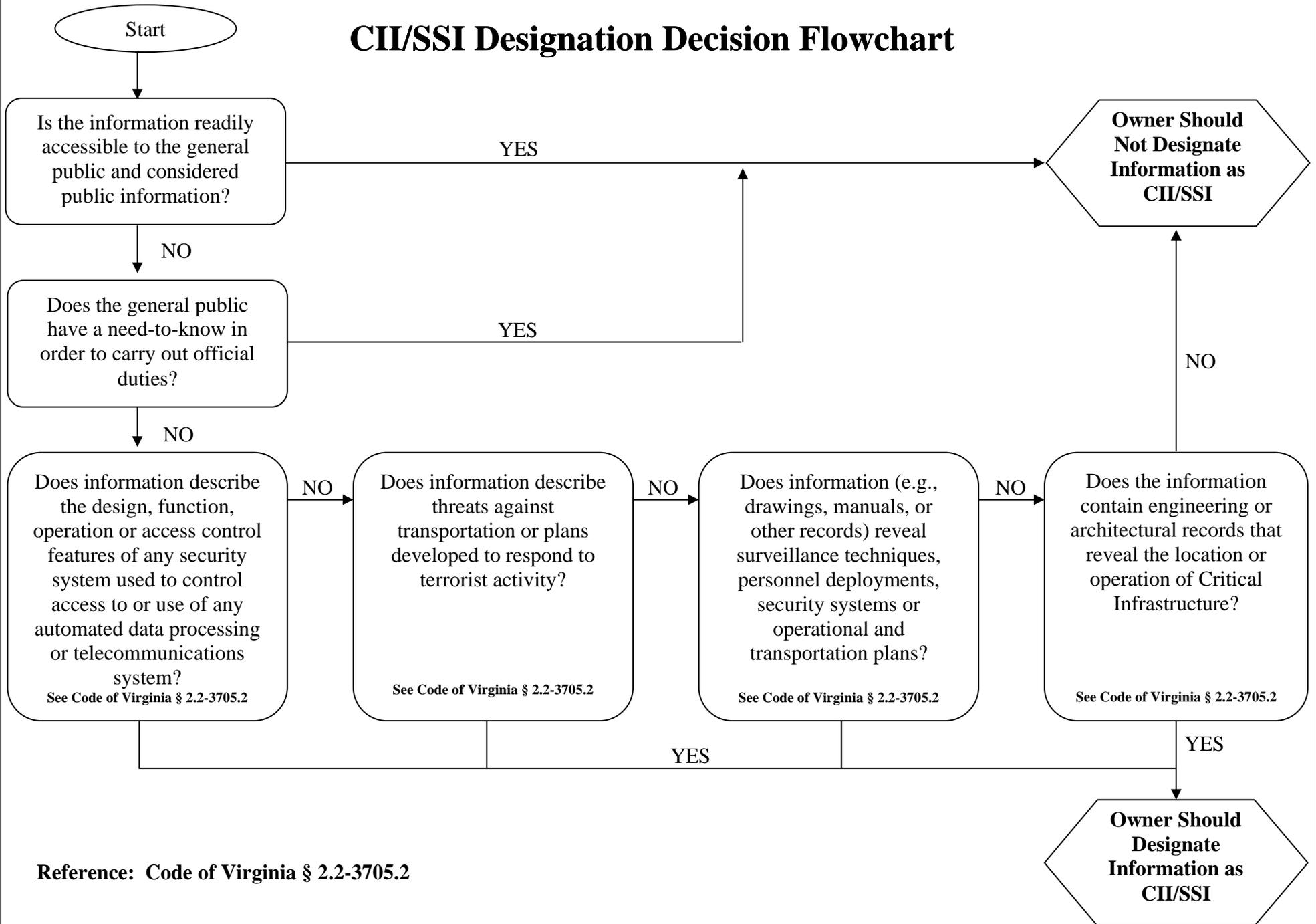
### Points to consider when determining what constitutes CII/SSI...

- What impact could the information have if it was inadvertently transferred to an unintended audience?
- Does the information provide details concerning security procedures and capabilities?
- Could someone use the information to target personnel, facilities or operations?
- How could someone intent on causing harm misuse the information?
- Could the use of this information be dangerous if combined with other publicly available information?
- Look at the material from an adversary's point of view.

	<b>Answer the following:</b>	<b>Y/N</b>
	Is the information customarily public knowledge? (Information that is accessible to the general public if there has been no deliberate attempt to keep it hidden or secret.)	
	Does the general public have a need-to-know? (Access to, or knowledge or possession of, specific information required to carry out official duties ) (Note: Contractors should be considered employees, not general public.)	
	If “yes” to either, then it is <b>not</b> CII/SSI, otherwise continue.	
<b>If the item under consideration shows describes or is itself listed below, it might be CII/SSI.</b>		
1	Documentation or other information that describes the design, function, operation or access control features of any security system, manual or automated, used to control access to or use of any automated data processing or telecommunications system.	
2	Plans and information to prevent or respond to terrorist activity, the disclosure of which would jeopardize the safety of any person, including: <ul style="list-style-type: none"> <li>• Critical infrastructure sector or structural components</li> <li>• Operational, procedural, transportation, and tactical planning or training manuals</li> <li>• Vulnerability assessments</li> <li>• Staff meeting minutes or other records</li> </ul> Engineering or architectural records or portions of, that reveals the location or operation of: <ul style="list-style-type: none"> <li>• Security equipment and systems</li> <li>• Elevator equipment and systems</li> <li>• Ventilation equipment and systems</li> <li>• Fire protection equipment and systems</li> <li>• Emergency equipment and systems</li> <li>• Electrical equipment and systems</li> <li>• Utility equipment and systems</li> <li>• Telecommunications equipment and systems</li> </ul>	
3	Information (including drawings, manuals, or other records) which reveals: <ul style="list-style-type: none"> <li>• Surveillance techniques</li> <li>• Alarm or security systems or technologies</li> <li>• Personnel deployments<sup>1</sup></li> <li>• Operational and transportation plans or protocols</li> </ul>	
4	Information concerning threats against transportation.	

<sup>1</sup> Only as it relates to security operations. (E.g. Staffing levels in critical operational areas such as Smart Traffic Centers, Control Rooms, Guard schedules, number present and location, etc.)

# CII/SSI Designation Decision Flowchart



**Reference: Code of Virginia § 2.2-3705.2**



## Critical Infrastructure Information/Sensitive Security Information (CII/SSI) Multi-Purpose Non-Disclosure Agreement

Retain a copy of both the front and back sides of this form for future reference

**VDOT requires CII/SSI be protected and not disclosed to unauthorized persons.**

### PART A: To Be Completed By Individual VDOT or Company Employee

**I agree with the following as a condition of being granted access to CII/SSI:**

*CII/SSI, which is valuable and sensitive, is protected by law and by strict VDOT policies. The intent of these laws and policies is to assure that CII/SSI will remain confidential - that is, it will be used only as necessary to accomplish VDOT's mission. Disclosure of CII/SSI in any manner that permits interception by unauthorized persons could compromise safety and security and is prohibited. CII/SSI may be released only to persons with a need-to-know.*

*exclusion from further VDOT related work; and legal liability. My obligations with respect to the confidentiality and security of all CII/SSI disclosed to me shall survive the termination of any agreement or relationship with VDOT. My execution of this agreement shall not nullify or affect in any manner any other agreement, non-disclosure or otherwise, which I have executed or may execute with VDOT or the Commonwealth of Virginia.*

*I might have access to this information in various formats including but not limited to documents and drawings, physical structures, and computer based systems. I have no right or ownership interest in any VDOT CII/SSI. VDOT may at any time revoke my authorization allowing access to CII/SSI.*

*I am obligated to protect this information from unauthorized disclosure in accordance with the terms of this agreement. I will only use CII/SSI that I obtain to perform my legitimate VDOT related duties. I will conduct myself in a strict conformance to applicable laws and VDOT policies governing CII/SSI. I will safeguard the confidentiality of all CII/SSI at all times. I will be responsible for my misuse or my wrongful disclosure of CII/SSI.*

*Willful violation of this agreement may subject me to discipline which might include, but is not limited to, removal from current VDOT projects;*

Each provision of this agreement is severable. If any administrative or judicial tribunal should find any provision of this agreement to be unenforceable, all other provisions shall remain in full force and effect.

I make this agreement in good faith, without mental reservation or purpose of evasion.

Printed Name	Date
VDOT District/Division OR Company Name	Phone Number
Company Address	
Signature	Signature of Authorized Agent <small>(Not required for VDOT employees)</small>

### PART B: To Be Completed By Company Agent Only:

**In addition to the provisions above, I certify:**

*All employees of this company involved with this VDOT project, regardless of location, who will have access to CII/SSI, myself included, will complete Part A of the Critical Infrastructure Information/Sensitive Security Information Multi-Purpose Non-Disclosure Agreement. The Agreement will be signed by me and accepted by VDOT prior to being granted access to CII/SSI. We will only access CII/SSI for which we have a need-to-know.*

*We will safeguard the confidentiality of all CII/SSI at all times. We will conduct ourselves in strict conformance to applicable laws and VDOT policies governing CII/SSI. Obligations with respect to the confidentiality and security of all CII/SSI disclosed to us shall survive the termination of any agreement or relationship with VDOT.*

Authorized Company Agent:

Signature of Authorized Agent	Date
Printed Name	Title
Company Name	Phone Number
Company Address	
VDOT Contract Name and Number	



**Critical Infrastructure Information/Sensitive Security Information (CII/SSI)  
Multi-Purpose Non-Disclosure Agreement**  
*Back Page*

Retain a copy of both the front and back sides of this form for future reference.

**Handling CII/SSI**

You are responsible for safeguarding Critical Infrastructure Information/Sensitive Security Information (CII/SSI) in your custody or under your control.

The extent of protection afforded CII/SSI shall be sufficient to reasonably foreclose the possibility of its loss or compromise.

The terms of this clause (*Handling CII/SSI*), including this paragraph, must be included in any dissemination of any document, in whole or in part, that contains CII/SSI.

Protection - CII/SSI shall be protected at all times, either by appropriate storage or having it under the personal observation and control of a person authorized to receive it. Each person who works with protected CII/SSI is personally responsible for taking proper precautions to ensure that unauthorized persons do not gain access to it.

Use and Storage - During working hours, reasonable steps shall be taken to minimize the risks of access to CII/SSI by unauthorized personnel. After working hours, CII/SSI shall be secured in a secure container, such as a locked desk, file cabinet or facility where contract security is provided.

Reproduction - Documents or material containing CII/SSI may be reproduced to the minimum extent necessary consistent with the need to carry out official duties provided that the reproduced material is marked and protected in the same manner as the original material.

Disposal - Material containing CII/SSI shall be disposed of by any method that prevents unauthorized retrieval (e.g. shredding, burning, returning to original source, etc.).

Transmission - CII/SSI shall be transmitted only by VDOT courier, US first class, express, certified or registered mail, or through secure electronic means.