Critical Infrastructure Information (CII)
Sensitive Security Information (SSI)
Individual Non-Disclosure Agreement

Code of Virginia §36-105.3 and §44-146.22 and 49 CFR Part 1520 stipulates instituting procedures to ensure the safe storage and secure handling of information that should be protected and not disclosed. VDOT CII/SSI includes such information and is not subject to disclosure under FOIA (reference Code of Virginia §2.2-3705.2).

Disclosure of CII/SSI in any manner that permits interception by unauthorized persons is prohibited. CII/SSI may not be released to persons without a need-to-know except with written permission from VDOT (see *Handling CII/SSI* on page 3). CII/SSI includes information marked as such or other information relating to VDOT security or protected systems (see *Guide to Identifying Possible CII* on page 4).

All documents and materials provided are the sole and exclusive property of VDOT. They may not be modified, reproduced, republished, redistributed or presented for sale, completely or in part, and doing so may result in severe civil and criminal penalties. All documents and materials provided are only to be used in conjunction with contract or project # _____.

As an employee of (or contractor to) _____ I understand that:

1. Certain information which I will receive from Virginia Department of Transportation (VDOT) may contain CII/SSI.
2. I may learn of or have access to some or all of this information through a computer system or through my employment activities.
3. CII/SSI is valuable and sensitive and 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.
4. I have no right or ownership interest in any CII/SSI referred to in this Agreement.
5. Willful violation of this agreement may subject me to discipline which might include, but is not limited to, termination of employment or further VDOT related work and to legal liability.
6. I am obligated to protect this information from unauthorized disclosure in accordance with the terms of this agreement.
7. Unauthorized disclosure of CII/SSI could compromise safety and security of persons and is prohibited.
8. 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.
9. 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.
10. I am required to conduct myself in a strict conformance to applicable laws and VDOT policies governing CII/SSI (see *Handling CII/SSI* on page 3).
11. VDOT may at any time revoke my authorization allowing access to CII/SSI.

Accordingly, as a condition of and in consideration of my access to CII/SSI, I agree that:

1. I will only access CII/SSI for which I have a need-to-know
2. I will use any CII/SSI that I obtain only as needed by me to perform my legitimate VDOT related duties.
3. I will not in any way divulge, copy, release, sell, loan, review, alter or destroy any CII/SSI except as properly authorized within the scope of my professional VDOT activities

Last Name, First name: _____

4. I will safeguard the confidentiality of all CII/SSI at all times.
5. I will safeguard and will not disclose my access code or any other authorization I have that allows me to access CII/SSI and I accept responsibility for all activities undertaken using my access code and other authorization.
6. I will be responsible for my misuse or my wrongful disclosure of CII/SSI and for my failure to safeguard my access code or other authorization access to CII/SSI.

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.
Please make sure to make a copy of your driver's license to send in with the form.
I make this agreement in good faith, without mental reservation or purpose of evasion.

Printed name of Individual Staff Member	Date
Company Name	Phone Number
Company Address	Fax Number
Company City, State, Zip	E-mail Address
Signature of Individual Staff Member	

Authorized Agent for Company (person who signed the Company Agreement):

Printed Name of Authorized Agent	Title
Signature of Authorized Agent	Phone Number
VDOT Contact Name	

Return copy of signed agreement to _____.

(Retain this page and the next for 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.

Critical Infrastructure Information (CII)
Sensitive Security Information (SSI)
Individual Non-Disclosure Agreement

Things to consider regarding the need to protect 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?

Before looking at the Guide, answer the following:

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 **not** CII/SSI otherwise, continue to the guide.	X

Guide to Identifying Possible CII/SSI		
If the item under consideration shows, describes or is listed below, it might be CII/SSI.		**Y/N**
1	Information, the disclosure of which would jeopardize the safety or security of any person or structure, including engineering and construction drawings and plans that reveal: • Critical structural components • Ventilation systems • Elevators • Mandatory building emergency equipment or systems • Security equipment and systems • Fire protection equipment • Telecommunications equipment and systems • Electrical systems • Other utility equipment and systems *(COV § 2.2-3705.2 (2))*	
2	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. *(COV § 2.2-3705.2 (3))*	
3	Plans and information to prevent or respond to terrorist activity, the disclosure of which would jeopardize the safety of any person, including: • Critical infrastructure sector or structural components • Vulnerability assessments • Operational, procedural, transportation, and tactical planning or training manuals • Staff meeting minutes or other records Engineering or architectural records or portions of, that reveals the location or operation of: • Security equipment and systems • Ventilation equipment and systems • Emergency equipment and systems • Utility equipment and systems • Elevator equipment and systems • Fire protection equipment and systems • Electrical equipment and systems • Telecommunications equipment and systems The same categories of records submitted to us for the purpose of antiterrorism response planning if accompanied, in writing, a statement that: • Invokes the protection of §2.2-3705.2 • Specifically identifies the records or portions thereof which are to be protected • States why the protection of such records from public disclosure is necessary *(COV § 2.2-3705.2 (4))*	
4	Information including (drawings, manuals, or other records) which reveals: • Surveillance techniques • Personnel deployments • Alarm or security systems or technologies • Operational and transportation plans or protocols *(COV § 2.2-3705.2 (6))*	
5	Information concerning threats against transportation. *(USC 49 CFR 1520 (5))*	