Office of Safety, Security & Emergency Management

CII / SSI Policy

Critical Infrastructure Information
Sensitive Security Information
Policy

Version 8
July 18, 2024

Policy Revision History

Version #	Effective Date
Version 1	September 1, 2003 (Initial Release)
Version 2	April 7, 2004
Version 3	August 1, 2004
Version 4	October 15, 2004
Version 5	April 15, 2005
Version 6	February 3, 2006
Version 7	November 2009 (Interim Revision)
Version 8	July 11, 2024 (Update)

Contents

I. Background 5
II. Purpose and Scope 5
III. Definitions 5
IV. References (additional information) 8
V. Policy Author 9
VI. Internal Reviewer 9
VII. Authorizing Officer 9
VIII. Effective Date 9
IX. Review Date 9
X. Policy Statements 9
XI. Exceptions 11
XII. Penalties 11

Refer to the CII/SSI Policy Guide for Employees, Vendors, Contractors or other Persons Accessing VDOT's CII/SSI for detailed information on the designation, marking, and handling of CII/SSI material.

This page intentionally left blank

VDOT Critical Infrastructure Information/Sensitive Security Information (CII/SSI) Policy

I. Background

The Office of Safety, Security & Emergency Management (OSSEM) at VDOT is responsible for ensuring the protection and security of specific information covered by two terms. This includes Critical Infrastructure Information (CII) as defined in 6 CFR Part 29 and the Homeland Security Act of 2002, Subtitle B of Title II, the Critical Infrastructure Information Act of 2002 (6 U.S.C. §§131), and Sensitive Security Information (SSI) as defined in Federal Code in 49 CFR Part 1520. For this policy, we collectively refer to this information as Critical Infrastructure Information/Sensitive Security Information (CII/SSI).

CII/SSI, regardless of its form (drawings, plans, text, cyber, etc.), should be afforded a level of protection against loss or unauthorized disclosure commensurate with its value and classification. CII/SSI security, like all security, should be considered in terms of risk management. Risk management factors to be considered include the sensitivity, value and critical nature of the infrastructure information; analysis of the known and anticipated threats and vulnerabilities; and countermeasures benefits versus cost.

II. Purpose and Scope

A. Purpose

To establish uniform procedures for the identification, classification and security protection of CII/SSI and to dictate how the CII/SSI is identified, marked, safeguarded, protected, used and stored, reproduced, disposed of, and transmitted.

B. Scope

The scope of this policy applies to all VDOT employees, individuals working on VDOT projects under a contract, subcontract, memorandum of understanding, or similar arrangement, or to any others needing access to VDOT's CII/SSI information.

Compliance with this policy is specifically the responsibility of the District Administrators and Division Administrators but application of the policy applies to everyone who has control over, access to, is in receipt of, or is responsible for the creation, care, storage, and proper marking of CII/SSI.

III. Definitions

A. Authorized Person - A person who, in the performance of official duties, has a need-to-know for information designated CII/SSI, has signed the proper non-disclosure agreement, and has been cleared for access to CII/SSI material through VDOT's Criminal History Records Check process as required in DPM: 1-25. (see Unauthorized Person, Unauthorized Access)

B. Critical Infrastructure (CI) - Critical Infrastructure means systems and assets, whether physical or virtual, so vital to the United States and Virginia that the incapacity or destruction of such systems and assets would have a debilitating impact on security, economic security, public health or safety, or any combination thereof.

C. Critical Infrastructure Information (CII) – A document designation, not a classification. This designation is used by VDOT to identify information or material (plans, drawings, reports etc.) which is not appropriate for public release without a need-to-know; information that is not customarily public knowledge and that the public would not generally need-to-know. CII consists of records or information related to the security of Critical Infrastructure or protected systems. This includes but is not limited to:

1. Actual, potential or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected system by physical or computer-based attack or other similar conduct, including the misuse of or unauthorized access to all types of communications and data transmission systems that violate Federal, State or local law, harms interstate commerce of the United States, or threatens the public health or safety;
2. The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit or;
3. Any planned or past operational problem or solution regarding critical infrastructure or protected system, including repair, recovery, reconstruction, insurance, or continuity to the extent it is related to such interference, compromise, or incapacitation.
4. Information which is excluded from the provisions of the Freedom of Information Act (FOIA) and exempt from public disclosure as information or records related to public safety pursuant to § 2.2- 3705.2 of the Code of Virginia, or any succeeding statute.

D. Critical Infrastructure Information/Sensitive Security Information Program (CII/SSI Program) - OSSEM Security program established for the development, management, maintenance, and review of procedures to be used to identify, classify, and protect Critical Infrastructure Information and Sensitive Security Information throughout VDOT.

E. Custodian – The employee charged with the responsibility of protecting the CII/SSI asset in accordance with the owner's specific instructions.

F. Due Care – Just, proper, and sufficient care, so far as the circumstances demand; the absence of negligence. That degree of care that a reasonable person can be expected to exercise. That care which an ordinarily prudent person would have exercised under the same or similar circumstances.

G. Fiduciary Responsibility – The legal relationship that gives rise to a duty to act on behalf of another with the highest standard of trust and good faith.

H. **Good Faith** - A state of mind consisting of faithfulness to one's duty or obligation; absence of intent to defraud or to seek unconscionable advantage.

I. **Maritime Facility** - Any structure or facility of any kind located in, on, under, or adjacent to any waters subject to the jurisdiction of the U.S. and used, operated, or maintained by a public or private entity, including any contiguous or adjoining property under common ownership or operation.

J. **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. Information that is intended for use only by individuals who require the information in the course of performing their job function.

K. **Operational Security** - A process to deny potential adversaries information about capabilities and/or intentions by identifying, controlling, and protecting sensitive information. Frequently referred to as Operational Security (OpSec). The CII/SSI policy integrates OpSec processes into the way VDOT protects its sensitive information.

L. **Owner** – One to assign the value of CII/SSI asset; a senior-level person who has been assigned to exercise the organization's proprietary rights and fiduciary responsibilities for the CII/SSI asset in question.

M. **Proprietary Rights** – Pertaining to property ownership and rights associated with ownership (i.e. possession, control, use).

N. **Protected System** – Protected system means any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of VDOT and includes any physical or computer-based system including a computer, computer system, computer or communications network, or any component hardware or element thereof, software programs, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage.

O. **Public Knowledge** – Information about which knowledge or use is accessible to the public if there has been no deliberate attempt to keep it hidden or secret. The 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 nonpublic 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.)

P. **Security-in-depth** – OSSEM security program consisting of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within a facility. Examples include, but are not limited to use of

employee, visitor, and contractor access controls; perimeter fences; use of intrusion detection systems (IDS); random guard patrols throughout facilities during working and non-working hours; closed circuit television surveillance; and other safeguards that mitigate the vulnerabilities of open storage areas without alarms and security storage containers, during working and non-working hours.

Q. **Sensitive Security Information (SSI)** – Sensitive Security Information is a document designation, not a classification. Material designated as SSI consists of information related to maritime facilities and must be protected from unauthorized disclosure to ensure transportation security as required by the Maritime Transportation Security Act of 2002.

R. **Unauthorized Access** - Unauthorized access means gaining access to or receiving CII/SSI without the proper authority to do so. (also unauthorized disclosure, unauthorized release, unauthorized retrieval, unauthorized use, unauthorized removal, unauthorized entry)

S. **Unauthorized Person** - A person not authorized to have access to CII/SSI or other sensitive information. (see Authorized Person)

IV. References (additional information)

Code of Virginia

- Code of Virginia § 2.2-3705.2 Exclusion to the application of chapter
- Code of Virginia § 44-146.22, Development of measures to prevent or reduce harmful consequences of disaster: disclosure of information.

Federal

- 6 CFR Part 29, Procedures for Handling Critical Infrastructure Information, Federal Register, Vol. 69, No. 34, February 20, 2003, pp 8074 – 8089
- 33 CFR Part 6, Protection and Security of Vessels, Harbors and Waterfront Facilities
- 33 CFR Part 101, Maritime Security: General
- 49 CFR Part 1520, Protection of Sensitive Security Information,
- US Patriot Act (Public Law 107–56) (Oct. 26, 2001)
- Homeland Security Act of 2002 (Public Law 107-296, 116 stat. 2135, sections 211215), Title II, Subtitle B, Section 214: Critical Infrastructure Information Act of 2002, 6 USC §§131-134
- Maritime Transportation Security Act (Public Law 107-295), 46 USC Part 2101,
- Presidential Decision Directive 63 (PDD 63) (May 22, 1998)
- Homeland Security Presidential Directive 7 (HSPD-7) (Dec. 17, 2003)
- Executive Order (EO) 13231, Critical Infrastructure Protection in the Information Age
- USCG Navigation and Vessel Inspection Circular 10 04, Guidelines for Handling Sensitive Security Information
- U.S. Department of Transportation, Security, and Emergency Preparedness Guide

Other

- National Industrial Security Program Operating Manual (NISPOM)
- VDOT HR Policy 2.10e
- DHRM Policy 1.60, Standards of Conduct
- VDOT DPM Number 1-25, Criminal History Records Check Policy

V. Policy Author

Office of Safety, Security & Emergency Management
Security Section (OSSEM)
(Former Office of Safety and Security)

VI. Internal Reviewer

Steve Weber
Assistant Director for Security

VII. Authorizing Officer

John Scrivani CEM
Director - Office of Safety, Security & Emergency Management

VIII. Effective Date

February 3, 2006 (Version 6)
Interim Revision – November 2009 (Version 7)
Update – July 17, 2024 (Version 8)

IX. Review Date

July 17, 2024

X. Policy Statements

Good-Faith Effort - In a good-faith effort, all individuals identified in II.B shall apply all statements of this policy.

Due Care of CII/SSI - Due care shall be exercised in fulfilling each of the requirements of this policy as stated in this section.

Identifying CII/SSI - All individuals identified in II.B, in a good faith effort, are responsible for identifying CII/SSI within their possession or control.

Marking CII - All material identified as CII shall be marked as follows:

- - Restricted - -
Critical Infrastructure Information

Marking SSI - All material identified as SSI shall be marked as follows:

- The markings are to appear on every page of the document

- Protective marking to appear at the top of the page: **Sensitive Security Information**
- Distribution limitation statement to appear at the bottom of the page:

  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 a civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and **1520.**

Safeguarding - All individuals identified in II.B are responsible for safeguarding and protecting CII/SSI within their possession or control.

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 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 and in accordance with the established records retention policy.

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

Releasing CII/SSI – CII/SSI is not subject to disclosure under FOIA (ref. Code of Virginia §2.2-3705.2, CII/SSI is subject to the security and protection stipulated herein and is to be released only on a need-to-know basis, non-disclosure agreements signed and the person receiving the CII/SSI material has been cleared to access the CII/SSI material through VDOT's Criminal History Records Check process as required by DPM: 1-25.

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

Reporting Unauthorized Disclosure - Anyone becoming aware of the disclosure of CII/SSI to an unauthorized person, the loss or suspected loss of CII/SSI information, or other violation of this policy, should promptly inform VDOT's Information Security Officer.

Freedom of Information (FOIA) Requests – Nothing in this policy is intended to allow individuals to circumvent or deny appropriate FOIA requests. Questions regarding FOIA requests related to CII/SSI will be directed to the local FOIA coordinator in the VDOT District/Division to which the requested information pertains.

FOIA questions about security assessments, systems, or other security information can be directed to OSSEM's FOIA coordinator.

Any questions about this policy can be sent to: criticalinfrastructure@vdot.virginia.gov

XI. Exceptions

OSSEM will address exceptions on a case-by-case basis.

XII. Penalties

Failure to comply with this policy may result in:

- Application of a Group II offense per DHRM Standards of Conduct policy (1.60), Section V, B, 2, a) Failure to follow a supervisor's instructions, perform assigned work, or otherwise comply with established written policy and/or e) Unauthorized use or misuse of state property or records, or
- Application of a Group III offense per DHRM Standards of Conduct policy (1.60), Section V, B, 3, d) Theft or unauthorized removal of state records, state property, or the property of other persons.