Treatment of Critical Infrastructure Information

Version 3.0 – October 14, 2014

Purpose – Promotion of compliance with Indiana's Access to Public Records Act exceptions for critical infrastructure information.

Scope – This policy applies to all critical infrastructure information handled by IDHS employees.

Responsibilities – Employees are responsible for adhering to this policy. Management officials are responsible for ensuring that all employees are aware of this policy and for consistently enforcing the policy.

Authority

1) The Indiana Access to Public Records Act, IC 5-14-3-1, et seq.

2) Indiana Commission on Public Records Record Series Number 2010-24

Definition

Indiana Commission on Public Records Record Series Number 2010-24 defines Critical Infrastructure Information Records (CII) as:

> Homeland security and counterterrorism records which may be intra-agency or interagency advisory or deliberative material (including material developed by a private contractor under a contract with a public agency). These may be expressions of opinion or of a speculative nature, and include:
>
> 1) administrative or technical information that would jeopardize a record keeping or security system,
>
> 2) computer programs, codes, filing systems, and other software,
>
> 3) portions of electronic maps entrusted to a public agency by a utility, and
>
> 4) school safety and security measures, plans, and systems, including emergency preparedness plans developed under 511 IAC 6.1-2-2.5.
>
> Records may include correspondence, reports, assessments, strategies, grant applications, drawings, specifications, plans, and risk planning documents in paper or electronic form, as further described in IC 5-14-3-4(b)(6), (10), (11), (18) and 19. Disclosure of these records may be affected by the previously listed statutes. Retention is based on a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack should records be improperly disclosed.

Retention and Safeguarding

- Retention: The Indiana Public Access Counselor has determined that Critical Infrastructure Information Records (CII) may be destroyed when outdated or replaced. Attachment I lists

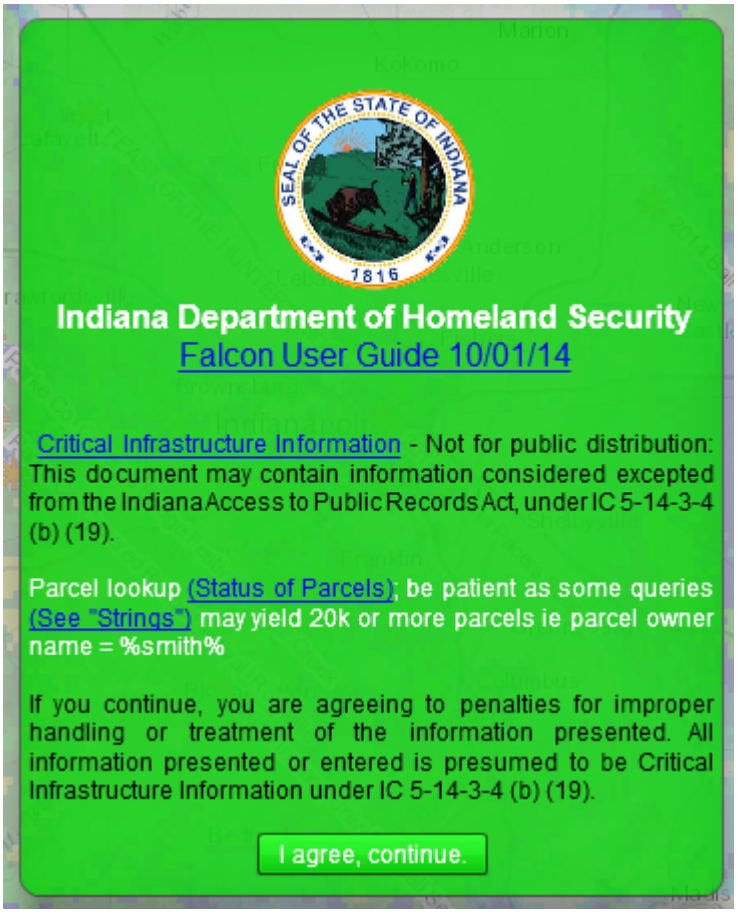
types and tiers of records that may be CII or may contain subsets of information that may be CII.

- Safeguarding: Attachment II lists handling options for various CII record types. Formats of CII considered for safekeeping include both paper and digital records. Suitable methods of safeguarding CII include cyber, procedural and physical approaches. Updates to Attachment II are anticipated since records comprising CII and technologies will evolve.

- Labeling: Physical records created by the agency that are, or contain, CII will include a cover sheet showing this emblem:

> **Critical Infrastructure Information - Not for public distribution:** This document contains information considered excepted from the Indiana Access to Public Records Act, under IC 5-14-3-4 (b) (19). Public disclosure of this record has a reasonable likelihood of threatening public safety by exposing vulnerabilities to terrorist attack.

- Labeling: Electronic records (web mapping applications) that are, or contain, CII will be labeled with a splash screen showing this emblem:



- Standard operating procedures will be updated on an as-needed basis, or at least reviewed on an annual basis.

Types of CII Records

- Submitted to IDHS by governmental entities: Records submitted to the agency as CII are to be treated as CII.
- Submitted to IDHS by private sector partner: Records submitted to the agency by members of the private sector as CII are to be treated as CII.
- Generated by IDHS: Attachment I lists types and tiers of records that may be CII or may contain subsets of information that may be CII.
- Images (electronic maps) that depict critical infrastructure, response activities and or plans are by definition CII data.

Distribution

- General Public: CII records are submitted to, or created by, the agency with the understanding that these records are not to become part of the public record. Distribution of CII to the general public is not allowed.
- Response Partners: CII records may be provided to public sector response partners on a need to know basis only when the intended recipients do not have standard operating procedures in place for treatment of CII. CII records may be provided to public sector response partners freely when the intended recipients do have standard operating procedures in place for treatment of CII, including provisions to safeguard CII received from IDHS. CII records may be provided to private sector response partners on a case-by-case basis to assure compliance with constraints on private, proprietary or trade-secret information.
- Requests either in person or by phone for CII records or enhanced access to CII records must be addressed within 24 hours. Or within seven days of receiving the request by mail or facsimile. Requests for CII records are to be immediately forwarded to the agency Public Information Officer for further action. Line and executive staff are not to handle these requests directly other than to pass the request(s) on to the Public Information Officer. Centralized handling of requests is necessary to assure consistency in responses and to avoid arbitrary or capricious behaviors in response to such requests.

ATTACHMENT I.

Types and tiers of records that may be CII or may contain subsets of information that may be CII.

CRITICAL INFRASTRUCTURE INFORMATION (CII)

- Homeland security and counterterrorism records which may be intra-agency or interagency advisory or deliberative material (including material developed by a private contractor under a contract with a public agency). These may be expressions of opinion or of a speculative nature, and include: 1) administrative or technical information that would jeopardize a record keeping or security system, 2) computer programs, codes, filing systems, and other software, 3) portions of electronic maps entrusted to a public agency by a utility, and 4) school safety and security measures, plans, and systems, including emergency preparedness plans developed under 511 IAC 6.1-2-2.5. Records may include correspondence, reports, assessments, strategies, grant applications, drawings, specifications, plans, and risk planning documents in paper or electronic form, as further described in IC 5-14-3-4(b)(6), (10), (11), (18) and 19. Disclosure of these records may be affected by the previously listed statutes. Retention is based on a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack should records be improperly disclosed.

RETENTION SCHEDULE FOR CII RECORDS in IDHS

- DESTROY when outdated or replaced.

Handling options for CII record types.

Record Type	Digital Records, publication - electronic documents, images, databases transmitted via web services
Best	Password protected service with (need to know) role-based access and user interface marked with "confidential and not subject to public disclosure under IC 5-14-3-4 without approval of (insert name of disseminating agency)". Accessed via VPN or within a closed network.
Minimum Requirement	Password protected service with (need to know) role based access and user interface marked with "confidential and not subject to public disclosure under IC 5-14-3-4 without approval of (insert name of disseminating agency)". Using https or equivalent encryption protocol.

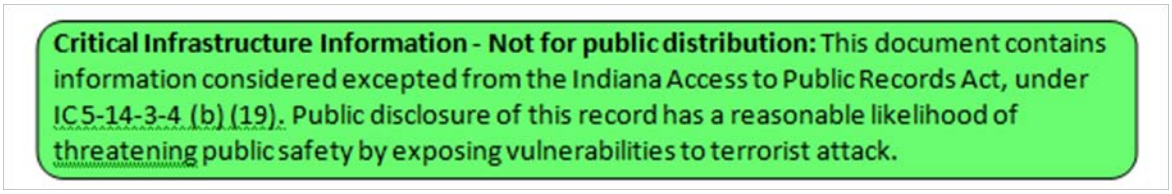
Record Type	Digital Records, files sent via email
Best	File attached to an email within a secure network like HSIN or HSDN; or upload of file via https to a portal like LENS or IDHS WebEOC.
Better	Encrypted password protected attachment on email with password sent in separate email.
Minimum Requirement	Password protected file attachment on email with password sent in separate email.

Record Type	Digital Records, file storage
Best	Password protected file on an encrypted and password protected device to prevent unauthorized access to file storage and unauthorized opening of file. Storage device in a controlled access area or behind at least one lock.
Better	Password protected file on a password protected device to prevent unauthorized access to file storage and unauthorized opening of file. Storage device in a controlled access area or behind at least one lock.
Minimum Requirement	Password protected file to prevent unauthorized opening of file. Storage device in a controlled access area or behind at least one lock.

Handling options for CII record types (cont'd).

Record Type	Paper Records, storage
Best	Storage in a locking container (file cabinet, desk) in a controlled access area and behind at least one locked door.
Better	Storage in a locking container (file cabinet, desk) behind at least one locked door.

Record Type	Paper Records, transmission via mail
	Double wrapped, envelope in an envelope. Inner envelope to be marked with:



With a request for unintended recipient to notify sender, return unopened contents promptly plus appropriate contact info and return address.

Retention of Records, (electronic or paper)

Destroy when outdated or replaced. Preference is not to store unneeded copies.