

보안취약점 협력대응제도 동향과 대응

부제 : A path towards Coordinated Vulnerability Disclosure(CVD)

2024. 6. 20

KISA, KrCERT/CC

이 태 승



목차

- ❑ CVD 소개 및 동향
- ❑ CVD 법제화 구성요소
- ❑ CVD 법제화 이슈사항

Q : What is CVD(Coordinated Vulnerability Disclosure) ?


- ✓ **Not yet heard**


- ✓ **Partially Relevant Answers**
 - CVE(Common Vulnerabilities & Exposures)
 - NVD(National Vulnerability Database)

- ✓ **Mostly Relevant Answer**
 - Bug Bounty

- ✓ **Mostly Correct Answers**
 - Vulnerability Disclosure Policy(VDP)
 - Responsible Disclosure

Origin of CVD

 Microsoft | MSRC [Report an issue](#) [Customer guidance](#) [Engage](#) [Who we are](#) [Blogs](#) [Acknowledgments](#)

 This blog post is older than a year. The information provided below may be outdated.

[Blog](#) / [2010](#) / [07](#) / [Coordinated-Vulnerability-Disclosure-Bringing-Balance-To-The-Force](#) /

Coordinated Vulnerability Disclosure: Bringing Balance to the Force

[BlueHat](#) / By [bluehat](#) / July 21, 2010 / 7 min read

Today on the [MSRC blog,](<http://blogs.technet.com/b/msrc/archive/2010/07/22/announcing-coordinated-vulnerability-disclosure.aspx> >) Matt Thomlinson, General Manager of Trustworthy Computing Security, announced our new philosophy on Coordinated Vulnerability Disclosure. I wanted to provide some context and history on how this came about. This post is about changing the way we at Microsoft talk about some familiar disclosure concepts, and is meant as an introduction to how Microsoft would like to engage with researchers. We're opening up a dialogue with the community here, and we welcome your feedback.

Responsible Disclosure (RD), Full Disclosure (FD) – everybody has an opinion, and each believes that their way is the best way to keep users safe. For background, one general definition of RD as most vendors define it is that the issue is reported privately to the vendor *and no one else* until the vendor issues a patch. In contrast, proponents of FD provide all vulnerability details to everyone at the same time, a move designed to make vendors provide updates faster.

Needless to say, most vendors including Microsoft are in favor of RD, while finders fall across the spectrum from FD to RD. Ultimately, we are all part of a virtual security team with the common goal of making the Internet safer and protecting the people using it – it's good to remind everyone that we're on the same team, and we should keep the dialogue open, even when we disagree.

The term Coordinated Vulnerability Disclosure was first introduced to me by Jake Kouns of [OpenSecurityFoundation.org](#), when we spoke at great length after I was on a panel at RSA on Responsible Disclosure. WeldPond (AKA Chris Wysopal, CTO of Veracode) recently [tweeted](#): *"We need to start calling working with the vendor 'Coordinated Disclosure'. I agree that 'Responsible' is too loaded."*

The concept of making the name more descriptive makes perfect sense to me, since the term "responsible" can be subjective to so many. Even the ISO draft standard that was originally titled "Responsible Vulnerability Disclosure" is now called "Vulnerability Disclosure," signaling that researchers, vendors, and (gasp!) even policy makers agree that the old term is more subjective.

The intention of RD was that it was designed to be a fair way to negotiate between researchers and vendors around vulnerability reporting and resolution. However, that has resulted in much debate, between vendors and finders. So, how do we move past this debate towards providing a better solution?

Source : Microsoft

What is CVD

Vulnerability Response Process

(대응 프로세스)

Coordinated Vulnerability Disclosure is the process of gathering information from vulnerability finders, coordinating the sharing of that information between relevant stakeholders, and disclosing the existence of software vulnerabilities and their mitigations to various stakeholders, including the public. CVD is an important aspect of any successful VR process. CVD inputs are vulnerability reports arising from vulnerability discovery practices. CVD outputs for product vulnerabilities

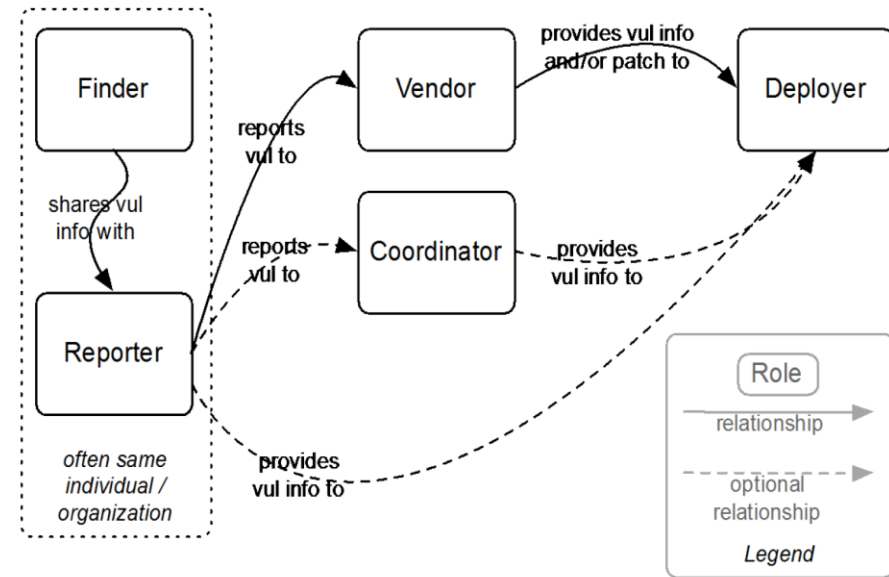


Figure 1: CVD Role Relationships

Source : SEI-CMU

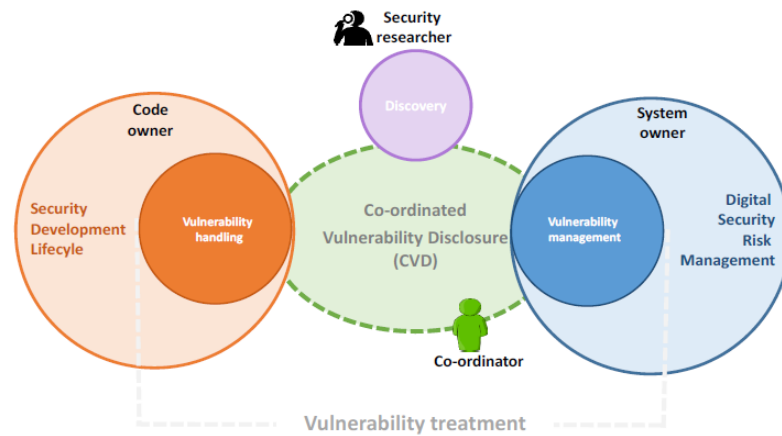
What is CVD

Vulnerability Disclosure Lifecycle

발견 → 신고 → 조치 → 공개

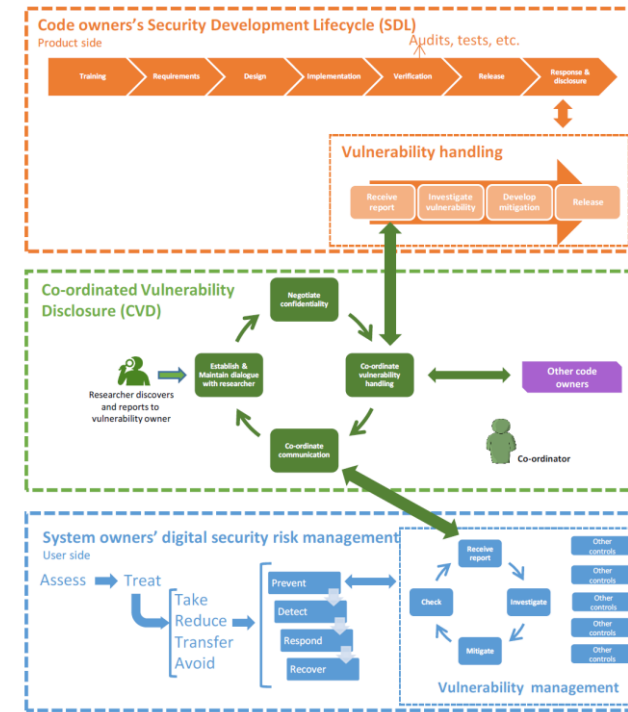
Figure 4. Vulnerability treatment

Vulnerability treatment = Discovery + Handling + Management + Co-ordination of disclosure (CVD)



Source: OECD

Figure 5. CVD as part of the broader product and system security



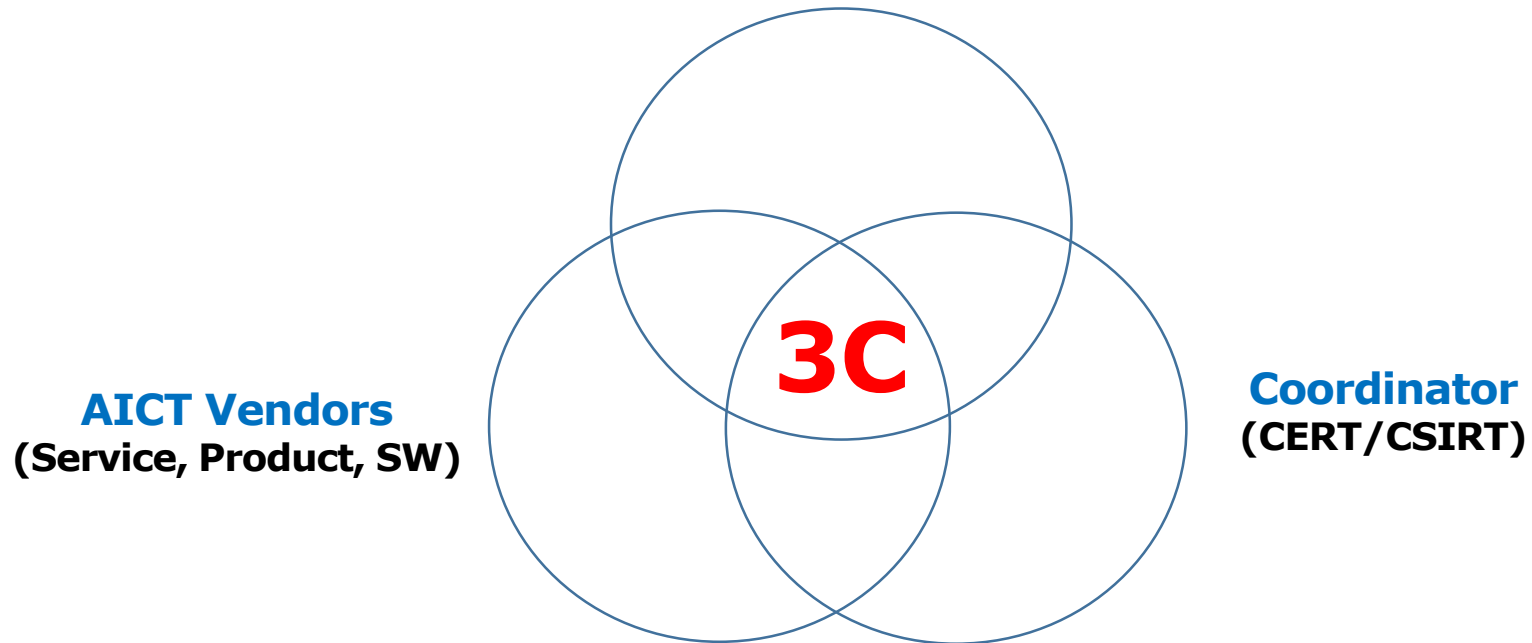
Source: OECD

'Coordinated' in CVD

3C

Communication(소통), **C**ooperation(협력), **C**oordination(조정)

Security/Vulnerability Researcher
(White-hat Hacker, etc.)



Source : Author(Presenter)

'Disclosure' in CVD

Reporting (신고), Provision (제공), Disclosure (공개)

1.1.4. Vulnerability disclosure

The meaning of "vulnerability disclosure" varies in the literature. Sometimes, the term covers the entire vulnerability lifecycle, from discovery to public disclosure, including some parts of vulnerability handling and management (1.1.5), which are inherently related to disclosure. "Vulnerability disclosure" can be used to refer to the provision of vulnerability information from one stakeholder to another, such as when a security researcher reports a vulnerability to a vulnerability owner or co-ordinator. It can also be used as an abbreviation for "public disclosure", i.e. the provision of vulnerability information to the public.

This imprecise use of the term is common in the technical community but can be confusing for the non-expert. It reveals that this area is still relatively nascent and rarely approached from a holistic perspective. Section 1.1.6 proposes the term "vulnerability treatment" to refer to the broad subject area.

In this document, the provision of vulnerability information to a vulnerability owner or co-ordinator is called "reporting".

This section introduces the types of vulnerability disclosure generally referred to in the literature, and describes the vulnerability disclosure lifecycle.

Types of vulnerability disclosure

Four types of vulnerability disclosure are often distinguished in the literature:

- *Non-disclosure*: vulnerability information is not disclosed to anyone.
- *Full disclosure*: vulnerability information is disclosed to the public unilaterally, i.e. without co-ordination.
- *Disclosure to third parties*: information is disclosed to other parties than those who can develop mitigations or assist in the development of a mitigation.
- *Limited disclosure*: the disclosure is limited in a manner that reduces risk to all parties, for instance to a vulnerability owner or co-ordinator, or to the public but with a low level of detail, and when mitigations are available.

Source : OECD

Why CVD is important

Cybersecurity towards CVD

	US	EU	OECD
Law, Regulation	FISMA 2014 IoT Cybersecurity Improvement Act of 2020	DIRECTIVE (EU) 2022/2555(NIS2) Cyber Resilience Act(CRA) Cybersecurity Act(CSA) AI Act	
Strategy, Policy	National Cybersecurity Strategy(NCS) EO 14028 Zero Trust Architecture SW Supply Chain Security Cyber Trust Mark Secure by Design EO 14110 : AI Roadmap OSS Security Policy	27 EU member states' strategies and policies	OECD Policy Framework on Digital Security
Guide, etc.	Vulnerability Response Playbook CVD Program NIST SP 800-216 NIST CSF 2.0 CFAA Policy 2022	ENISA Reports on CVD EU CSIRTs Network for CVD	OECD Guides on CVD

CVD in US (1/12)



FISMA 2014

IoT Cybersecurity Improvement Act of 2020

National Cybersecurity Strategy(NCS)

EO 14028

Zero Trust Architecture

SW Supply Chain Security

Cyber Trust Mark

Secure by Design

EO 14110 : AI Roadmap

OSS Security Policy

Vulnerability Response Playbook

CVD Program

NIST SP 800-216

NIST CSF 2.0

CFAA Policy 2022




EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

September 2, 2020

M-20-32

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Russell T. Vought 
Director

SUBJECT: Improving Vulnerability Identification, Management, and Remediation

Background

This memorandum provides Federal agencies with guidance for obtaining and managing their vulnerability research programs. Implementation will allow for the security research community (“reporters”) to report vulnerability information to appropriate agency contacts, who can then use the reports to mitigate associated risks of which they may not have been aware.

Federal agencies have begun integrating coordinated vulnerability disclosure (CVD) methodologies into their cybersecurity risk management programs. These CVD initiatives seek to identify security risks by enabling members of the public conducting security research with an avenue to safely report security vulnerabilities they uncover on Federal information systems.¹ OMB applauds these efforts, and Federal agencies should continue to align their CVD programs with internationally recognized standards² to the extent possible, consistent with Federal law and policy. CVD can expand the diversity of thinking involved in vulnerability identification and substantively improve the cybersecurity posture of Federal information systems.

Source : OMB

CVD in US (2/12)

US

FISMA 2014

IoT Cybersecurity Improvement Act of 2020

National Cybersecurity Strategy(NCS)

EO 14028

Zero Trust Architecture

SW Supply Chain Security

Cyber Trust Mark

Secure by Design

EO 14110 : AI Roadmap

OSS Security Policy

Vulnerability Response Playbook

CVD Program

NIST SP 800-216

NIST CSF 2.0

CFAA Policy 2022

- **Clearly Worded VDP:** Agency VDPs shall clearly articulate which systems are in scope and the set of security research activities that can be performed against them to protect those who would report vulnerabilities. Federal agencies shall provide clear assurances that good-faith security research⁵ is welcomed and authorized.
- **Clearly Identified Reporting Mechanism:** Each Federal agency shall clearly and publicly identify where and how Federal information system vulnerabilities should be reported.
- **Timely Feedback:** Federal agencies shall provide timely feedback to good-faith vulnerability reporters. Once a vulnerability is reported, those who report them deserve to know they are being taken seriously and that action is being taken. Agencies should establish clear expectations for regular follow-up communications with the vulnerability reporter, to include an agency-defined timeline for coordinated disclosure.
- **Unencumbered Remediation:** To streamline communication and collaboration, Federal agencies shall ensure vulnerability reports are available to system owners within 48 hours of submission, and shall establish a channel for system owners to communicate with vulnerability reporters, as appropriate.
- **Good-Faith Security Research is Not an Incident or Breach:** Good-faith security research does not itself constitute an incident or breach under the Federal Information Security Modernization Act of 2014 (FISMA) or OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*. However, in the process of assessing and responding to vulnerabilities reported according to agencies' VDPs, agencies shall work with their senior agency officials for privacy (SAOPs) to evaluate affected Federal information systems for breaches that occurred outside the scope of the good-faith security research (e.g., a breach that occurred before the research was conducted) and follow the requirements outlined in M-17-12. Pursuant to M-17-12, agencies may impose stricter standards consistent with their missions, authorities, circumstances, and identified risks.

Source : OMB M-20-32

CVD in US (3/12)

US

Regulations based on FISMA
IoT Cybersecurity Improvement Act of 2020

National Cybersecurity Strategy(NCS)

EO 14028

- Zero Trust Architecture
- SW Supply Chain Security
- Cyber Trust Mark
- Secure by Design
- EO 14110 : AI Roadmap
- OSS Security Policy

Vulnerability Response Playbook

- CVD Program
- NIST SP 800-216
- NIST CSF 2.0
- CFAA Policy 2022

BINDING OPERATIONAL DIRECTIVES

BOD 19-02: Vulnerability Remediation Requirements for Internet-Accessible Systems

April 29, 2019

RELATED TOPICS: CYBERSECURITY BEST PRACTICES



This page contains a web-friendly version of Operational Directive 19-02, "Vulnerability Remediation Requirements for Internet-Accessible Systems".

A binding operational directive is a purpose of safeguarding federal information and information systems.

[Section 3553\(b\)\(2\) of title 44, U.S. Code](#), authorizes the Secretary of the Department of Homeland Security (DHS) to develop and oversee the implementation of binding operational directives.

Federal agencies are [required](#) to comply with DHS developed directives.

These directives [do not apply](#) to statutory defined "national security systems" nor to certain systems operated by the Department of Defense or the Intelligence Community.

BINDING OPERATIONAL DIRECTIVES

BOD 20-01: Develop and Publish a Vulnerability Disclosure Policy

September 02, 2020

RELATED TOPICS: CYBERSECURITY BEST PRACTICES



This page contains a web-friendly version of Operational Directive 20-01, "Develop and Publish a Vulnerability Disclosure Policy".

A binding operational directive is a purpose of safeguarding federal information and information systems.

[Section 3553\(b\)\(2\) of title 44, U.S. Code](#), authorizes the Secretary of the Department of Homeland Security (DHS) to develop and oversee the implementation of binding operational directives.

Federal agencies are [required](#) to comply with DHS developed directives.

These directives [do not apply](#) to statutory defined "national security systems" nor to certain systems operated by the Department of Defense or the Intelligence Community.

BINDING OPERATIONAL DIRECTIVES

BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities

November 03, 2021

RELATED TOPICS: CYBERSECURITY BEST PRACTICES



This page contains a web-friendly version of the Cybersecurity and Infrastructure Security Agency's Binding Operational Directive 22-01 - Reducing the Significant Risk of Known Exploited Vulnerabilities.

A binding operational directive is a [compulsory direction](#) to federal, executive branch, departments and agencies for purposes of safeguarding federal information and information systems.

[Section 3553\(b\)\(2\) of title 44, U.S. Code](#), authorizes the Secretary of the Department of Homeland Security (DHS) to develop and oversee the implementation of binding operational directives.

Federal agencies are [required](#) to comply with DHS developed directives.

These directives [do not apply](#) to statutory defined "national security systems" nor to certain systems operated by the Department of Defense or the Intelligence Community.

Source : CISA

CVD in US (4/12)

US

Regulations based on FISMA
IoT Cybersecurity Improvement Act of 2020

National Cybersecurity Strategy(NCS)

- EO 14028
- Zero Trust Architecture
- SW Supply Chain Security
- Cyber Trust Mark**
- Secure by Design
- EO 14110 : AI Roadmap
- OSS Security Policy

Vulnerability Response Playbook

- CVD Program
- NIST SP 800-216
- NIST CSF 2.0
- CFAA Policy 2022

PUBLIC LAW 116-207—DEC. 4, 2020 134 STAT. 1005

SEC. 6. IMPLEMENTATION OF COORDINATED DISCLOSURE OF SECURITY VULNERABILITIES RELATING TO AGENCY INFORMATION SYSTEMS, INCLUDING INTERNET OF THINGS DEVICES.

Consultation. 15 USC 278g-3d.

Deadline.

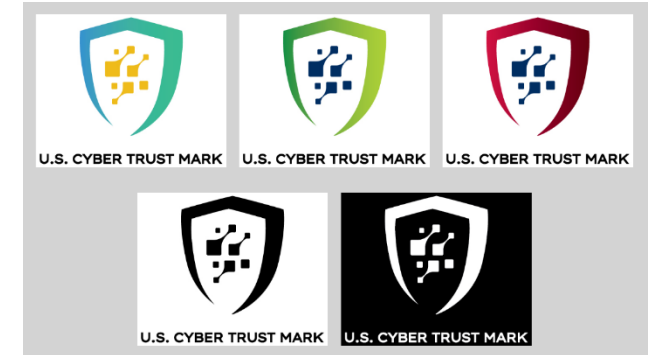
(a) AGENCY GUIDELINES REQUIRED.—Not later than 2 years after the date of the enactment of this Act, the Director of OMB, in consultation with the Secretary, shall develop and oversee the implementation of policies, principles, standards, or guidelines as may be necessary to address security vulnerabilities of information systems (including Internet of Things devices).

(b) OPERATIONAL AND TECHNICAL ASSISTANCE.—Consistent with section 3553(b) of title 44, United States Code, the Secretary, in consultation with the Director of OMB, shall provide operational and technical assistance to agencies on reporting, coordinating, publishing, and receiving information about security vulnerabilities of information systems (including Internet of Things devices).

(c) CONSISTENCY WITH GUIDELINES FROM NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.—The Secretary shall ensure that the assistance provided under subsection (b) is consistent with applicable standards and publications developed by the Director of the Institute.

(d) REVISION OF FEDERAL ACQUISITION REGULATION.—The Federal Acquisition Regulation shall be revised as necessary to implement the provisions under this section.

SEC. 7. CONTRACTOR COMPLIANCE WITH COORDINATED DISCLOSURE OF SECURITY VULNERABILITIES RELATING TO AGENCY INTERNET OF THINGS DEVICES. 15 USC 278g-3e.



Source : IoT Cybersecurity Improvement Act of 2020

Source : FCC

CVD in US (5/12)

US

Regulations based on FISMA IoT Cybersecurity Improvement Act of 2020

National Cybersecurity Strategy(NCS)

EO 14028

Zero Trust Architecture
SW Supply Chain Security
Cyber Trust Mark
Secure by Design

EO 14110 : AI Roadmap

OSS Security Policy

Vulnerability Response Playbook

CVD Program

NIST SP 800-216

NIST CSF 2.0

CFAA Policy 2022

- **Good-Faith Security Research is Not an Incident or Breach:** Good-faith security research does not itself constitute an incident or breach under the Federal Information Security Modernization Act of 2014 (FISMA) or OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*. However, in the process of assessing and responding to vulnerabilities reported according to agencies' VDPs, agencies shall work with their senior agency officials for privacy (SAOPs) to evaluate affected Federal information systems for breaches that occurred outside the scope of the good-faith security research (e.g., a breach that occurred before the research was conducted) and follow the requirements outlined in M-17-12. Pursuant to M-17-12, agencies may impose stricter standards consistent with their missions, authorities, circumstances, and identified risks.

Source : OMB M-20-32

Department of Justice Announces New Policy for Charging Cases under the Computer Fraud and Abuse Act

Thursday, May 19, 2022

Share >

For Immediate Release

Office of Public Affairs

The Department of Justice today announced the

[revision of its policy](#) regarding charging violations of the Computer Fraud and Abuse Act (CFAA).

The policy for the first time directs that good-faith security research should not be charged. Good faith security research means accessing a computer solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in a manner designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices, machines, or online services to which the accessed computer belongs, or those who use such devices, machines, or online services.

Source : DOJ

CVD in US (6/12)



Regulations based on FISMA
IoT Cybersecurity Improvement Act of 2020

- National Cybersecurity Strategy(NCS)**
- EO 14028**
- Zero Trust Architecture**
- SW Supply Chain Security**
- Cyber Trust Mark**
- Secure by Design**
- EO 14110 : AI Roadmap**
- OSS Security Policy**
- Vulnerability Response Playbook**
- CVD Program**
- NIST SP 800-216**
- NIST CSF 2.0**
- CFAA Policy 2022**

Pillar Three: Shape Market Forces to Drive Security and Resilience

- 3.2 **Drive the Development of Secure IoT Devices**
 - 3.2.1 Implement Federal Acquisition Regulation (FAR) requirements per the Internet of Things (IoT) Cybersecurity Improvement Act of 2020
 - 3.2.2 Initiate a U.S. Government IoT security labeling program
- 3.3 **Shift Liability for Insecure Software Products and Services**
 - 3.3.1 Explore approaches to develop a long-term, flexible, and enduring software liability framework
 - 3.3.2 Advance software bill of materials (SBOM) and mitigate the risk of unsupported software
 - 3.3.3 Coordinated vulnerability disclosure
- 3.4 **Use Federal Grants and Other Incentives to Build in Security**
 - 3.4.1 Leverage Federal grants to improve infrastructure cybersecurity
 - 3.4.2 Prioritize funding for cybersecurity research
 - 3.4.3 Prioritize cybersecurity research, development, and demonstration on social, behavioral, and economic research in cybersecurity
- 3.5 **Leverage Federal Procurement to Improve Accountability**
 - 3.5.1 Implement Federal Acquisition Regulation (FAR) changes required under EO 14028
 - 3.5.2 Leverage the False Claims Act to improve vendor cybersecurity
- 3.6 **Explore a Federal Cyber Insurance Backstop**
 - 3.6.1 Assess the need for a Federal insurance response to a catastrophic cyber event

Source : The White House



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

January 26, 2022

M-22-09

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young *Shalanda D. Young*
Acting Director

SUBJECT: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

D. Applications and Workloads

Vision

Agencies treat all applications as internet-connected, routinely subject their applications to rigorous empirical testing, and welcome external vulnerability reports.

Actions

1. Agencies must operate dedicated application security testing programs.
2. Agencies must utilize high-quality firms specializing in application security for independent third-party evaluation.
 - CISA and GSA will work together to make the services of such firms available for rapid procurement.
3. Agencies must maintain an effective and welcoming public vulnerability disclosure program for their internet-accessible systems.

Source : OMB

CVD in US (7/12)

US

Regulations based on FISMA
IoT Cybersecurity Improvement Act of 2020

National Cybersecurity Strategy(NCS)

EO 14028

Zero Trust Architecture
SW Supply Chain Security
Cyber Trust Mark
Secure by Design

EO 14110 : AI Roadmap

OSS Security Policy

Vulnerability Response Playbook

CVD Program

NIST SP 800-216

NIST CSF 2.0

CFAA Policy 2022



6. **Publish a vulnerability disclosure policy.** Publish a vulnerability disclosure policy that (1) authorizes testing against all products offered by the manufacturer and conditions for those tests, (2) provides legal safe harbor for actions performed consistent with the policy, and (3) allows public disclosure of vulnerabilities after a set timeline. Manufacturers should perform root-cause analysis of discovered vulnerabilities and, to the greatest extent feasible, take actions to eliminate entire vulnerability classes. See CISA's [Vulnerability Disclosure Policy Template](#) for reference language.

Source : CISA

CVD in US (8/12)

US

Regulations based on FISMA
IoT Cybersecurity Improvement Act of 2020
Computer Fraud and Abuse Act (CFAA)

National Cybersecurity Strategy(NCS)

EO 14028

Zero Trust Architecture
SW Supply Chain Security
Cyber Trust Mark
Secure by Design

EO 14110 : AI Roadmap
OSS Security Policy

Vulnerability Response Playbook

CVD Program
NIST SP 800-216
NIST CSF 2.0
CFAA Policy 2022

OBJECTIVE 2.5 | Drive adoption of strong vulnerability management practices for AI systems.

CISA will develop tools and techniques to harden and test AI systems, as well as incorporate appropriate outputs of adversarial ML processes and AI system vulnerabilities into the [National Vulnerability Database](#). This includes conducting an operational test of an AI vulnerability in the [Coordinated Vulnerability Disclosure \(CVD\)](#) process, as well as writing strategic guidance for security testing and red teaming AI systems and software, particularly [Open Source Software](#).

Source : CISA Roadmap for AI

Objective 4.4. Foster OSS Vulnerability Disclosure and Response

CISA will continue to coordinate vulnerability disclosure and response for OSS vulnerabilities by leveraging relationships with the OSS community. This coordination may include establishing processes to specifically look for upstream issues in open source packages that critical infrastructure organizations depend on and quickly notify affected users of the identified vulnerabilities.

Source : CISA OSS Security Roadmap

CVD in US (9/12)

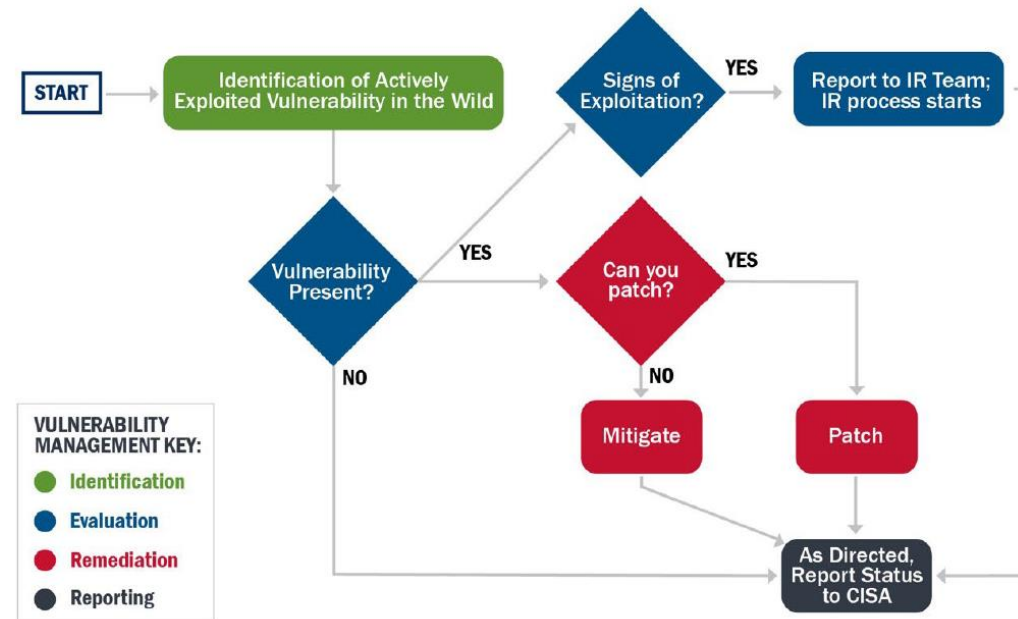
US

Regulations based on FISMA
 IoT Cybersecurity Improvement Act of 2020
 Computer Fraud and Abuse Act (CFAA)

- National Cybersecurity Strategy(NCS)
- EO 14028
- Zero Trust Architecture
- SW Supply Chain Security
- Cyber Trust Mark
- Secure by Design
- EO 14110 : AI Roadmap
- OSS Security Policy

Vulnerability Response Playbook

- CVD Program
- NIST SP 800-216
- NIST CSF 2.0
- CFAA Policy 2022



Source : CISA

CVD in US (10/12)

US

Regulations based on FISMA
IoT Cybersecurity Improvement Act of 2020
Computer Fraud and Abuse Act (CFAA)

National Cybersecurity Strategy(NCS)
EO 14028
Zero Trust Architecture
SW Supply Chain Security
Cyber Trust Mark
Secure by Design
EO 14110 : AI Roadmap
OSS Security Policy

Vulnerability Response Playbook

CVD Program
NIST SP 800-216
NIST CSF 2.0
CFAA Policy 2022

Coordinated Vulnerability Disclosure Process

CISA's CVD program coordinates the remediation and public disclosure of newly identified cybersecurity vulnerabilities in products and services with the affected vendor(s). This includes new vulnerabilities in industrial control systems (ICS), Internet of Things (IoT), and medical devices, as well as traditional information technology (IT) vulnerabilities. The goal of CISA's CVD program is to ensure that CISA, the affected vendor(s) and/or service provider(s), and the vulnerability reporter all disclose simultaneously, to ensure that users and administrators receive clear and actionable information in a timely manner.

Process

The CISA coordinated vulnerability disclosure process involves five basic steps:

- 1. Collection:** CISA collects vulnerability reports in three ways: CISA vulnerability analysis, monitoring public sources of vulnerability information, and direct reports of vulnerabilities to CISA. After receiving a report, CISA performs an initial analysis to assess a vulnerability's presence and compare with existing reports to identify duplicates. CISA then catalogs the vulnerability report, including all information that is known at that point.
- 2. Analysis:** Once the vulnerability reports are catalogued, vendor(s) and CISA analysts work to understand the vulnerabilities by examining the technical issue and the potential risk the vulnerability represents.
- 3. Mitigation Coordination:** After analyzing a vulnerability, CISA will continue to work with the affected vendor(s) for mitigation development and the issuance of patches or updates.
- 4. Application of Mitigation:** When possible and where necessary, CISA may work with vendor(s) to facilitate sufficient time for affected end users to obtain, test, and apply mitigation strategies prior to public disclosure.
- 5. Disclosure:** In coordination with the source of the vulnerability report and the affected vendor(s), CISA will take appropriate steps to notify users about the vulnerability via multiple channels. CISA strives to disclose accurate, neutral, objective information focused on technical remediation and mitigation for asset owners and operators. CISA will make references to available related information and correct misinformation where necessary.

Disclosure Timeline

Time frames for mitigation development and the type and schedule of disclosure may be affected by various factors. Extenuating circumstances, such as active exploitation, threats of an especially serious nature, or situations that require changes to established standards may result in changes to the disclosure timeline. Other factors include, but are not limited to:

- whether the vulnerability has already been publicly disclosed, i.e. published by a researcher;
- potential impact to critical infrastructure, national security, or public health and safety;
- the availability of effective mitigations;
- vendor responsiveness and feasibility of developing an update or patch;
- vendor estimate of time required for customers to obtain, test and apply the patch.

Source : CISA

CVD in US (11/12)

US

Regulations based on FISMA
 IoT Cybersecurity Improvement Act of 2020
 Computer Fraud and Abuse Act (CFAA)

National Cybersecurity Strategy(NCS)

- EO 14028
- Zero Trust Architecture
- SW Supply Chain Security
- Cyber Trust Mark
- Secure by Design
- EO 14110 : AI Roadmap
- OSS Security Policy

Vulnerability Response Playbook

- CVD Program
- NIST SP 800-216**
- NIST CSF 2.0
- CFAA Policy 2022

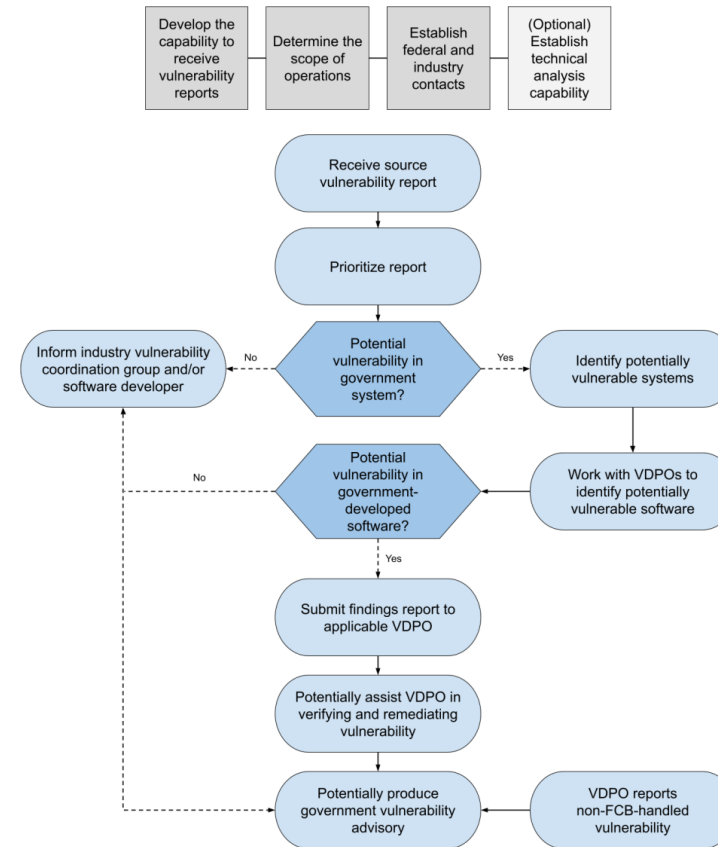


Fig. 2. Federal vulnerability disclosure coordination process

Source : NIST

CVD in US (12/12)

US

Regulations based on FISMA
IoT Cybersecurity Improvement Act of 2020
Computer Fraud and Abuse Act (CFAA)

National Cybersecurity Strategy(NCS)

EO 14028

Zero Trust Architecture

SW Supply Chain Security

Cyber Trust Mark

Secure by Design

EO 14110 : AI Roadmap

OSS Security Policy

Vulnerability Response Playbook

CVD Program

NIST SP 800-216

NIST CSF 2.0

CFAA Policy 2022

- **Risk Assessment (ID.RA):** The cybersecurity risk to the organization, assets, and individuals is understood by the organization
 - **ID.RA-01:** Vulnerabilities in assets are identified, validated, and recorded

18

NIST CSWP 29
February 26, 2024

The NIST Cybersecurity Framework (CSF) 2.0

- **ID.RA-02:** Cyber threat intelligence is received from information sharing forums and sources
- **ID.RA-03:** Internal and external threats to the organization are identified and recorded
- **ID.RA-04:** Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded
- **ID.RA-05:** Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization
- **ID.RA-06:** Risk responses are chosen, prioritized, planned, tracked, and communicated
- **ID.RA-07:** Changes and exceptions are managed, assessed for risk impact, recorded, and tracked
- **ID.RA-08:** Processes for receiving, analyzing, and responding to vulnerability disclosures are established
- **ID.RA-09:** The authenticity and integrity of hardware and software are assessed prior to acquisition and use
- **ID.RA-10:** Critical suppliers are assessed prior to acquisition

Source : NIST

CVD in EU (1/9)

EU

DIRECTIVE (EU) 2022/2555(NIS2)
 Cyber Resilience Act(CRA)
 Cybersecurity Act(CSA)
 AI Act

27 EU member states'
strategies and policies

ENISA Reports on CVD
EU CSIRTs Network for CVD

CHAPTER II

COORDINATED CYBERSECURITY FRAMEWORKS

Article 7

National cybersecurity strategy

1. Each Member State shall adopt a national cybersecurity strategy that provides for the strategic objectives, the resources required to achieve those objectives, and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include:
 - (a) addressing cybersecurity in the supply chain for ICT products and ICT services used by entities for the provision of their services;
 - (b) on the inclusion and specification of cybersecurity-related requirements for ICT products and ICT services in public procurement, including in relation to cybersecurity certification, encryption and the use of open-source cybersecurity products;
 - (c) managing vulnerabilities, encompassing the promotion and facilitation of coordinated vulnerability disclosure under Article 12(1);
2. As part of the national cybersecurity strategy, Member States shall in particular adopt policies:

Source : NIS2

CVD in EU (2/9)

EU

DIRECTIVE (EU) 2022/2555(NIS2)

Cyber Resilience Act(CRA)

Cybersecurity Act(CSA)

AI Act

**27 EU member states'
strategies and policies**

**ENISA Reports on CVD
EU CSIRTs Network for CVD**

Article 12

Coordinated vulnerability disclosure and a European vulnerability database

1. Each Member State shall designate one of its CSIRTs as a coordinator for the purposes of coordinated vulnerability disclosure. The CSIRT designated as coordinator shall act as a trusted intermediary, facilitating, where necessary, the interaction between the natural or legal person reporting a vulnerability and the manufacturer or provider of the potentially vulnerable ICT products or ICT services, upon the request of either party. The tasks of the CSIRT designated as coordinator shall include:

- (a) identifying and contacting the entities concerned;
- (b) assisting the natural or legal persons reporting a vulnerability; and
- (c) negotiating disclosure timelines and managing vulnerabilities that affect multiple entities.

Member States shall ensure that natural or legal persons are able to report, anonymously where they so request, a vulnerability to the CSIRT designated as coordinator. The CSIRT designated as coordinator shall ensure that diligent follow-up action is carried out with regard to the reported vulnerability and shall ensure the anonymity of the natural or legal person reporting the vulnerability. Where a reported vulnerability could have a significant impact on entities in more than one Member State, the CSIRT designated as coordinator of each Member State concerned shall, where appropriate, cooperate with other CSIRTs designated as coordinators within the CSIRTs network.

Source : NIS2

CVD in EU (3/9)

EU

DIRECTIVE (EU) 2022/2555(NIS2) Cyber Resilience Act(CRA) Cybersecurity Act(CSA) AI Act

27 EU member states' strategies and policies

ENISA Reports on CVD
EU CSIRTs Network for CVD

Intro | Events | Frequently Asked Question - FAQ | CVD

The European Union CSIRTs network is a network composed of EU Member States' appointed CSIRTs and CERT-EU ("CSIRTs network members"). The European Commission participates in the network as an observer.

The EU CSIRTs network was established in 2016 by a set of EU cybersecurity rules commonly referred to as the NIS Directive. In 2023, the CSIRTs network was further strengthened by the NIS2 Directive in order to contribute to the development of confidence and trust and to promote swift and effective operational cooperation among Member States.

ENISA is powering the CSIRTs network by providing the Secretariat team, infrastructures and tools to enable effective cooperation and continuous daily operation and information sharing.

The mission of the European Union CSIRTs network includes to:

- exchange information and build trust at EU level
- discuss and, where possible, implement a coordinated response to an incident
- provide EU Member States with assistance in addressing cross-border incidents
- cooperate and exchange best practices in incident response
- provide assistance to the CSIRTs designated for the coordinated disclosure of vulnerabilities which could have a significant impact on entities in more than one EU Member State.

CSIRTs NETWORK MEMBERS

Search by country or CSIRT Team

Constituency

- Government
- National
- Private and Public Sectors
- Private and Public Sectors
- Private and Public Sectors
- Government & military
- SP Customer Base
- Other

Vulnerability Disclosure Policies

Country	Organisation	Language	CNA	Policy/Reporting
BE	CCB	EN	No	Vulnerability reporting to the CCB (15 February 2023)
BE	CCB	FR	No	Signalement des vulnérabilités au CCB (15 février 2023)
DE	CERT-Bund	DE	No	Leitlinie und Richtlinie für Sicherheitsforschende (Dezember 2022)
DE	CERT-Bund	EN	No	BSI CVD guideline for security researchers (December 2022)
ES	INCIBE-CERT	EN	Yes	Vulnerability disclosure policy
ES	INCIBE-CERT	ES	Yes	CVE Assignment and publication
EU	ENISA	EN	Yes	ENISA Coordinated Vulnerability Disclosure Policy
EUI	CERT-EU	EN	No	Coordinated vulnerability disclosure policy
FI	NCSC-FI	EN	Yes	Vulnerability Coordination and Reporting
FR	ANSSI	FR	No	Vous souhaitez déclarer une faille de sécurité ?
NL	NCSC-NL	EN	Yes	Coordinated Vulnerability Disclosure: the Guideline (02 October 2018)
PL	CERT-PL	EN	Yes	Reporting vulnerabilities to CERT Polska
SK	SK-CERT	EN	Yes	Vulnerability Reporting Guideline (07 October 2019)
LU	CIRCL	EN	No	Responsible Vulnerability Disclosure (October 2019)
LV	CERT-LV	EN	No	Responsible Vulnerability Disclosure (September 2019)

Source : csirtsnetwork.eu

CVD in EU (4/9)

EU

DIRECTIVE (EU) 2022/2555(NIS2)
Cyber Resilience Act(CRA)
 Cybersecurity Act(CSA)
AI Act

27 EU member states' strategies and policies

ENISA Reports on CVD
 EU CSIRTs Network for CVD

CHAPTER II

OBLIGATIONS OF ECONOMIC OPERATORS

Article 10

Obligations of manufacturers

I. When placing a product with digital elements on the market, manufacturers shall ensure that it has been designed, developed and produced in accordance with the essential requirements set out in Section 1 of Annex I.

Manufacturers shall determine the expected product lifetime referred to in the first subparagraph of this paragraph taking into account the time users reasonably expect to be able to use the product with digital elements given its functionality and intended purpose and therefore can expect to receive security updates.

Manufacturers shall have appropriate policies and procedures, including coordinated vulnerability disclosure policies, referred to in Section 2, point (5), of Annex I, to process and remediate potential vulnerabilities in the product with digital elements reported from internal or external sources.

Security updates, referred to in Section 2, point (8), of Annex I, which have been made available to users shall remain available for a minimum duration of 10 years.

~~6. When placing a product with digital elements on the market, and for the expected product lifetime or for a period of five years from the placing of the product on the market, whichever is shorter, Manufacturers shall ensure, when placing a product with digital elements on the market and for a period of time after the placing on the market appropriate to the type of and its for the expected product lifetime, that vulnerabilities of that product, including its components, are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I.~~

Manufacturers shall have appropriate policies and procedures, including coordinated vulnerability disclosure policies, referred to in Section 2, point (5), of Annex I, to process and remediate potential vulnerabilities in the product with digital elements reported from internal or external sources.

Security updates, referred to in Section 2, point (8), of Annex I, which have been made available to users shall remain available for a minimum duration of 10 years.

Source : EU CRA draft

CVD in EU (5/9)

EU

DIRECTIVE (EU) 2022/2555(NIS2)
Cyber Resilience Act(CRA)
 Cybersecurity Act(CSA)
AI Act

27 EU member states'
 strategies and policies

ENISA Reports on CVD
 EU CSIRTs Network for CVD

Article 11

Reporting obligations of manufacturers

1. The manufacturers shall, ~~without undue delay,~~ notify **any actively exploited vulnerability contained in the product with digital elements that they become aware of** to the CSIRTs designated as coordinators pursuant to Article 12(1) of Directive (EU) 2022/2555, in accordance with paragraph 2b of this Article. ~~and in any event within 24 hours of~~
 - 1a. For the purpose of the notification referred to in paragraph 1, the manufacturers shall submit:
 - (a) Without undue delay and in any event within 24 hours of becoming aware of the actively exploited vulnerability, an early warning which shall provide general information, as available, about the product with digital elements concerned, the nature of the exploit and of the respective vulnerability. The early warning shall also indicate, where applicable, the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available. Where applicable, the early warning shall also indicate any corrective or mitigating measures taken, corrective or mitigating measures that users can take, and include an indication of how sensitive the manufacturer deems the notified information to be.

Source : EU CRA draft

CVD in EU (6/9)

EU

DIRECTIVE (EU) 2022/2555(NIS2)
Cyber Resilience Act(CRA)
 Cybersecurity Act(CSA)
AI Act

27 EU member states'
 strategies and policies

ENISA Reports on CVD
 EU CSIRTs Network for CVD

Article 8

High-risk AI systems

1. **Without prejudice to the requirements relating to accuracy and robustness set out in Article [Article 15] Products with digital elements classified as high-risk AI systems in accordance with Article [Article 6] of Regulation [the AI Regulation], products with digital elements which fall within the scope of this Regulation, and which are classified as high-risk AI systems pursuant to Article [Article 6] of Regulation [the AI Regulation] and fulfil the essential requirements set out in Section 1 of Annex I of this Regulation, and where the processes put in place by the manufacturer are compliant with the essential requirements set out in Section 2 of Annex I, shall be deemed in compliance with the cybersecurity requirements related to cybersecurity set out in Article [Article 15] of that Regulation [the AI Regulation], without prejudice to the other requirements related to accuracy and robustness included in the aforementioned Article, and in so far as the achievement of the level of protection required by those requirements is demonstrated by the EU declaration of conformity issued under this Regulation. if:**
 - (a) **they fulfil the essential requirements set out in Section 1 of Annex I to this Regulation;**
 - (b) **the processes put in place by the manufacturer are compliant with the essential requirements set out in Section 2 of Annex I to this Regulation; and**
 - (c) **the achievement of the level of cybersecurity protection required under Article [Article 15] of Regulation [the AI Regulation] is demonstrated in the EU declaration of conformity issued under this Regulation.**

Source : EU CRA draft

CVD in EU (7/9)

EU

DIRECTIVE (EU) 2022/2555(NIS2)
Cyber Resilience Act(CRA)
Cybersecurity Act(CSA)
 AI Act

27 EU member states'
 strategies and policies

ENISA Reports on CVD
 EU CSIRTs Network for CVD

7.6.2019

EN

Official Journal of the European Union

L 151/15

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 17 April 2019

on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

(Text with EEA relevance)

Article 6

Capacity-building

1. ENISA shall assist:
 - (a) Member States in their efforts to improve the prevention, detection and analysis of, and the capability to respond to cyber threats and incidents by providing them with knowledge and expertise;
 - (b) Member States and Union institutions, bodies, offices and agencies in establishing and implementing vulnerability disclosure policies on a voluntary basis;

CVD in EU (8/9)

EU

DIRECTIVE (EU) 2022/2555(NIS2)
Cyber Resilience Act(CRA)
Cybersecurity Act(CSA)
AI Act

**27 EU member states'
strategies and policies**

ENISA Reports on CVD
EU CSIRTs Network for CVD



Cyber Security Strategy for Germany 2021

8.1.8 Responding responsibly to vulnerabilities - promoting coordinated vulnerability disclosure

Why is the objective relevant?

Fixing known vulnerabilities quickly in systems, products and service provision is a cornerstone of cyber security. A user who discovers a vulnerability should contact the manufacturer of the product in question or the provider of the service in question immediately and in confidence, so that vulnerabilities that are detected can be fixed with a patch or update within a reasonable time period. There must be careful consideration of whether the vulnerability should be made public knowledge before the relevant updates or patches are available. Putting these factors into practice in a coordinated process is known as coordinated vulnerability disclosure (CVD).

Source : Federal Ministry of the Interior, Building and Community

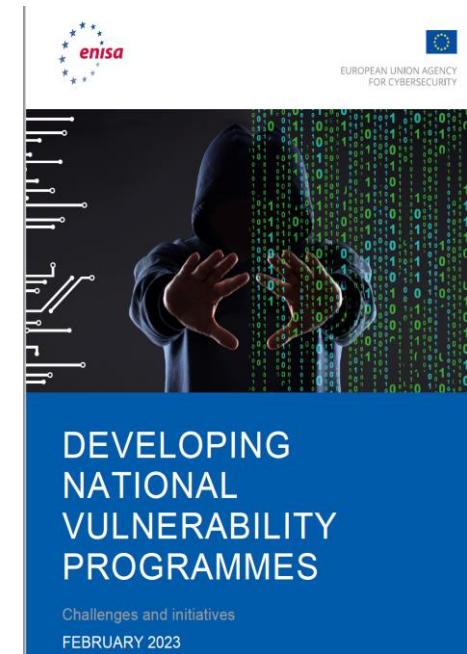
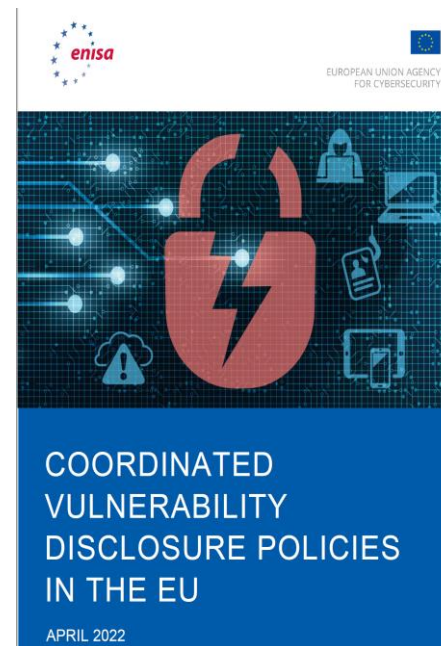
CVD in EU (9/9)

EU

DIRECTIVE (EU) 2022/2555(NIS2)
Cyber Resilience Act(CRA)
Cybersecurity Act(CSA)
AI Act
Directive 2013/40/EU (cybercrime)

27 EU member states'
strategies and policies

ENISA Reports on CVD
EU CSIRTs Network for CVD



Source : ENISA

CVD in OECD(1/2)

OECD

OECD Policy Framework on Digital Security



Note: the Cryptography Policy Guidelines which are currently under review, and Recommendation on Electronic Authentication, will be included in the future version of the draft Framework.
Source: OECD

CVD in OECD (2/2)

OECD

OECD Guides on CVD



Organisation for Economic Co-operation and Development

DSTI/CDEP/SDE(2020)3/FINAL

Unclassified

English - Or. English

3 February 2021

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INNOVATION
COMMITTEE ON DIGITAL ECONOMY POLICY

Working Party on Security in the Digital Economy

ENCOURAGING VULNERABILITY TREATMENT

Responsible management, handling and disclosure of vulnerabilities



Organisation for Economic Co-operation and Development

DSTI/CDEP/SDE(2021)9/FINAL

Unclassified

English - Or. English

25 January 2023

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INNOVATION
COMMITTEE ON DIGITAL ECONOMY POLICY

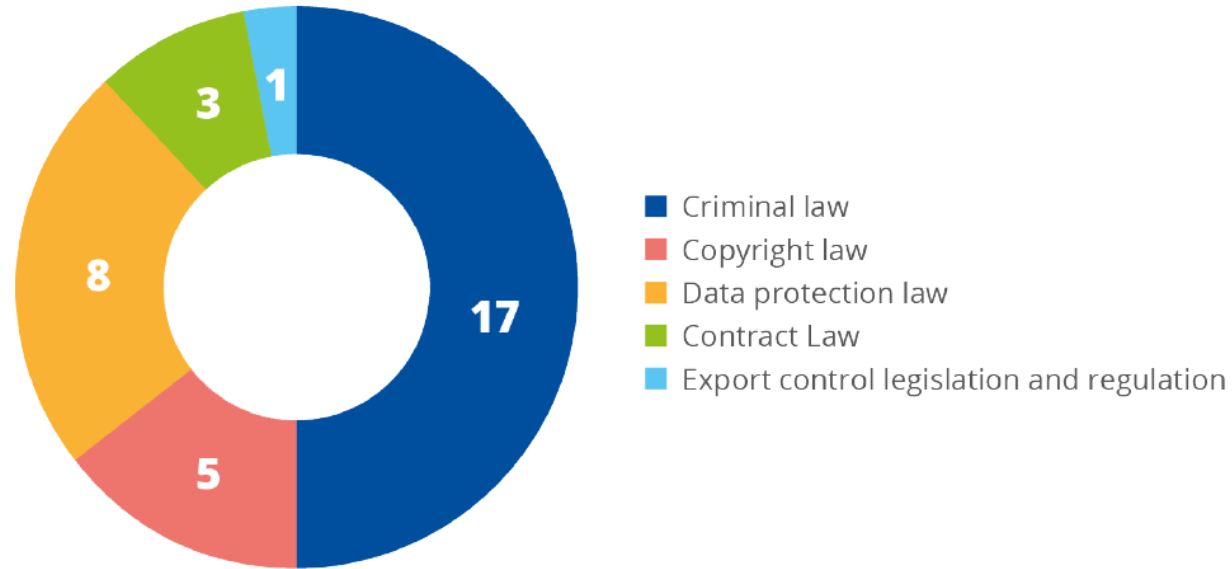
Working Party on Security in the Digital Economy

Good Practice Guidance on the Co-ordination of Digital Security Vulnerabilities

CVD challenges : safe harbor(1/4)

Figure 8 – Impact of the legal barriers in establishing a CVD policy

Which of the following legal barriers do you consider more impactful in the establishment of a CVD policy?



Source: Interviews with EU Member States

Source : ENISA

CVD challenges : safe harbor(2/4)

“good faith security research” means accessing a computer solely for purposes of good faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in a manner designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security of safety of the class of devices, machines, or online services to which the accessed computer belongs, or those who use such devices, machines, or online services.

Source : DOJ

CVD challenges : safe harbor(3/4)

- **Clearly Worded VDP:** Agency VDPs shall clearly articulate which systems are in scope and the set of security research activities that can be performed against them to protect those who would report vulnerabilities. Federal agencies shall provide clear assurances that good-faith security research⁵ is welcomed and authorized.
- **Clearly Identified Reporting Mechanism:** Each Federal agency shall clearly and publicly identify where and how Federal information system vulnerabilities should be reported.
- **Timely Feedback:** Federal agencies shall provide timely feedback to good-faith vulnerability reporters. Once a vulnerability is reported, those who report them deserve to know they are being taken seriously and that action is being taken. Agencies should establish clear expectations for regular follow-up communications with the vulnerability reporter, to include an agency-defined timeline for coordinated disclosure.
- **Unencumbered Remediation:** To streamline communication and collaboration, Federal agencies shall ensure vulnerability reports are available to system owners within 48 hours of submission, and shall establish a channel for system owners to communicate with vulnerability reporters, as appropriate.
- **Good-Faith Security Research is Not an Incident or Breach:** Good-faith security research does not itself constitute an incident or breach under the Federal Information Security Modernization Act of 2014 (FISMA) or OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*. However, in the process of assessing and responding to vulnerabilities reported according to agencies' VDPs, agencies shall work with their senior agency officials for privacy (SAOPs) to evaluate affected Federal information systems for breaches that occurred outside the scope of the good-faith security research (e.g., a breach that occurred before the research was conducted) and follow the requirements outlined in M-17-12. Pursuant to M-17-12, agencies may impose stricter standards consistent with their missions, authorities, circumstances, and identified risks.

Source : OMB M-20-32

CVD challenges : safe harbor(4/4)

<p>France</p>	<p>France has an established CVD policy. Art 47 (art. L 2321-4 Code de la défense) creates a safe harbour for vulnerability reporters when certain legal criteria are met.</p>	<p>Implemented</p>
<p>The Netherlands</p>	<p>The Netherlands has an established CVD policy that guarantees full protection for researchers.</p>	<p>Implemented</p>

Source : ENISA

CSR, Cybersecurity
CVD, Cybersecurity, Ethical hackers, Safe Harbour

Vulnerability reporting in Belgium: A safe harbour for ethical hackers

Published on **16/03/2023**

Source : www.headmind.com

CVD challenges : VDP 수립 및 공개 (1/2)

[표 14] 취약점처리방침(VDP) 주요 내용 [43]

구분	내용
공개 위치	· 홈페이지 (예 : https://.../vulnerability-disclosure-policy)
관련법 준수	· 취약점 발견 · 신고 · 처리 · 정보공개에 영향을 미치는 관련법 준수
허용 범위	· 취약점 발견이 허용된 제품, 시스템, 서비스 범위
허용 방법	· 취약점 발견 시 허용된 방법 · 디도스 공격, 사회 공학적 공격 등은 금지 · 개인정보 유출 금지 · 개인정보 발견 시 취약점 발견 시험 중단 · 제품, 시스템, 서비스 장애 발생 방지 노력
신고 방법	· 취약점 발견시 즉시 신고 · 취약점 신고 채널(이메일, 웹) · 익명 신고 허용
신고 정보	· 취약점 정보 · 취약점 발견 위치 · 취약점이 제품, 시스템, 서비스에 미치는 영향 등
법적 책임	· 취약점처리방침을 준수할 경우 민형사상 책임 면제 선언
취약점 처리 및 공개	· 신고된 취약점에 대한 처리 및 공개 절차 · 신고자가 요구하는 외부 공개 전까지의 기간
취약점처리방침 관리	· 취약점처리방침 공개 일자 · 취약점처리방침 이력 관리
포함해서는 안되는 내용	· 신고자의 개인정보 요구 · 취약점 정보를 일정 기한 이후에도 외부에 공개하는 것을 금지

Source : 일상 속 권리로 다가온 사이버보안(KISA Insight 2024 Vol.03)

CVD challenges : VDP 수립 및 공개(2/2)



The screenshot shows the official website of the U.S. Department of Commerce, specifically the Vulnerability Disclosure Policy page. The browser address bar displays the URL: <https://www.commerce.gov/vulnerability-disclosure-policy>. The page header includes the U.S. Department of Commerce logo and the text "U.S. Department of Commerce". A search bar is visible on the right side of the header. The main navigation menu includes links for "ABOUT", "ISSUES", "NEWS", "DATA AND REPORTS", and "WORK WITH US". The page content is divided into two columns. The left column contains a list of links: "Our mission", "Meet the Secretary", "Leadership", "Bureaus and offices", "Strategic Plan", "Equity", "Budget and performance", "Combined Federal Campaign", "COVID-19 Information Hub", and "History". The right column features the heading "Home" and the main title "Vulnerability Disclosure Policy". Below the title is an "Introduction" section with the following text: "The United States (U.S.) Department of Commerce (DOC) manages data critical to creating conditions for U.S. economic growth and opportunity. The DOC is committed to ensuring the security of the U.S. public by protecting the public's information from unwarranted disclosure. As such, the DOC has created a Vulnerability Disclosure Policy (VDP) and Vulnerability Disclosure Program, to give security researchers clear guidelines for conducting vulnerability discovery activities on DOC systems and websites and convey the DOC's preferences in how to submit discovered vulnerabilities to the DOC. The DOC's Vulnerability Disclosure Policy describes what systems and types of research are covered under this program, how to submit vulnerability reports, and requirements for public disclosure of submitted vulnerabilities."

Source : www.commerce.gov/vulnerability-disclosure-policy

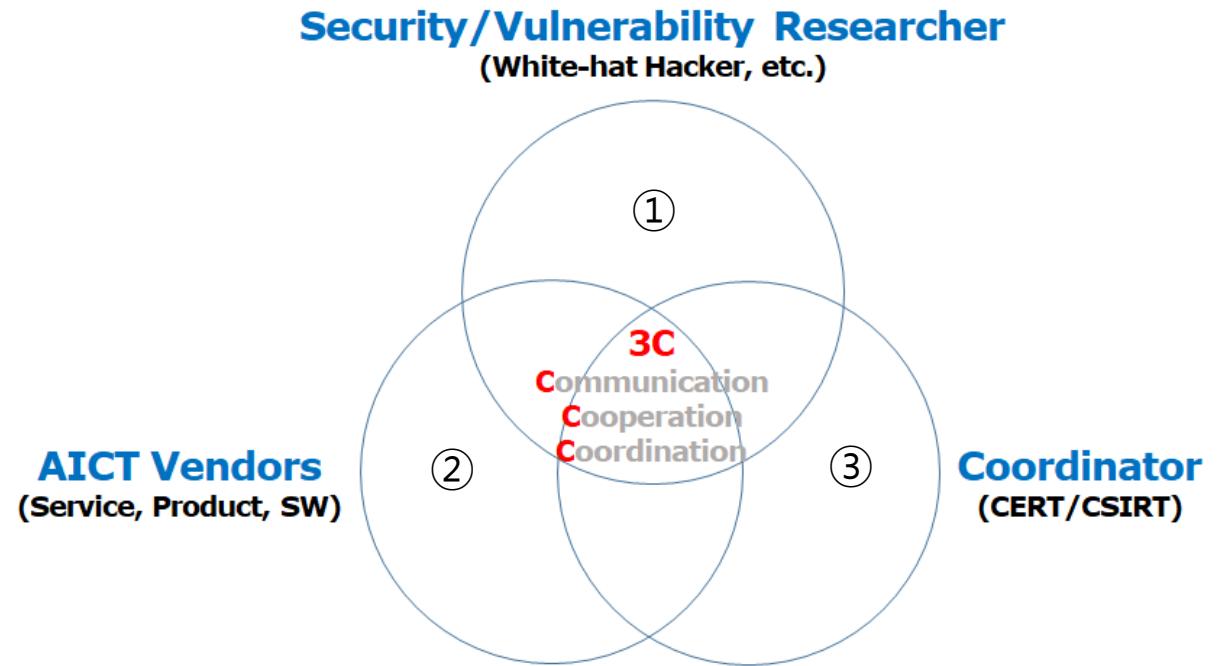
CVD challenges : Vuln. Disclosure

Window of Exposure

Weaponization

CVD 법제화 구성요소

- ① 보안연구자 법적 보호
 - 선의(**good-faith**)의 보안 연구 : **VDP** 준수
- ② 보안취약점 처리 방침(**VDP**) 수립·공개
 - 관련법 준수
- ③ **CVD** 운영기관(**coordinator**) 지정
 - 지원 및 조정
 - 보안취약점 신고 및 통지
 - 보안취약점 조치 및 공개



Source : Author(Presenter)

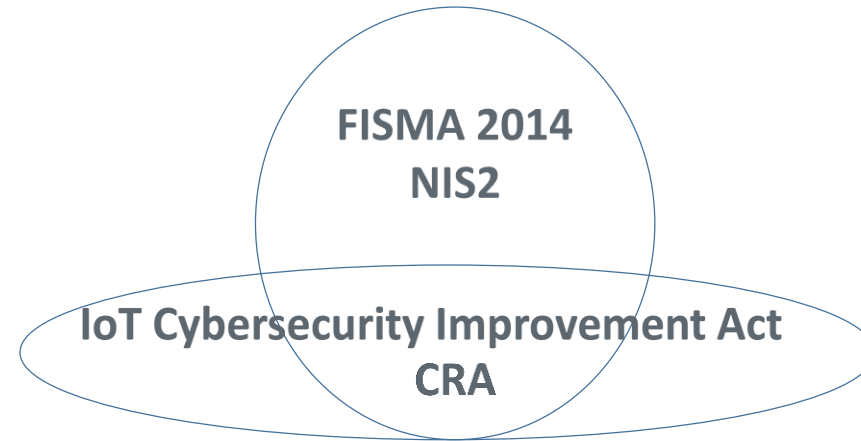
CVD 법제화 이슈사항 : 법체계

CVD scope

**Service
(provider)**

**Product, SW
(manufacturer,
distributor,
importer)**

Cybersecurity Law



Source : Author(Presenter)

CVD 법제화 이슈사항 : 정보통신망법 준수

제48조(정보통신망 침해행위 등의 금지)

- ① 누구든지 **정당한 접근권한 없이 또는 허용된 접근권한을 넘어** 정보통신망에 침입하여서는 아니된다.



선의의 보안 연구(VDP 준수)

CVD 법제화 이슈사항 : 개인정보보호법 준수

제59조(금지행위) **개인정보를 처리하거나 처리하였던 자**는 다음 각 호의 어느 하나에 해당하는 행위를 하여서는 아니 된다. <개정 2023. 3. 14.>

1. 거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 처리에 관한 동의를 받는 행위
2. 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공하는 행위
3. **정당한 권한 없이 또는 허용된 권한을 초과하여** 다른 사람의 개인정보를 **이용, 훼손, 멸실, 변경, 위조 또는 유출**하는 행위



선의를 보안 연구(VDP 준수)

CVD 법제화 이슈사항 : 저작권법 준수

저작권법 제104조의2(기술적 보호조치의 무력화 금지) ① **누구든지 정당한 권한 없이 고의 또는 과실로** 제2조제28호가목의 기술적 보호조치를 제거·변경하거나 우회하는 등의 방법으로 무력화하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.

1. 암호 분야의 연구에 종사하는 자가 저작물등의 복제물을 정당하게 취득하여 저작물등에 적용된 암호 기술의 결함이나 취약점을 연구하기 위하여 필요한 범위에서 행하는 경우. 다만, 권리자로부터 연구에 필요한 이용을 허락받기 위하여 상당한 노력을 하였으나 허락을 받지 못한 경우로 한정한다.
4. 국가의 법집행, 합법적인 정보수집 또는 안전보장 등을 위하여 필요한 경우
6. 정당한 권한을 가지고 프로그램을 사용하는 자가 다른 프로그램과의 호환을 위하여 필요한 범위에서 프로그램코드역분석을 하는 경우
7. **정당한 권한을 가진 자가** 오로지 **컴퓨터 또는 정보통신망의 보안성을 검사·조사** 또는 보정하기 위하여 필요한 경우
8. 기술적 보호조치의 무력화 금지에 의하여 특정 종류의 저작물등을 정당하게 이용하는 것이 불합리하게 영향을 받거나 받을 가능성이 있다고 인정되어 대통령령으로 정하는 절차에 따라 문화체육관광부장관이 정하여 고시하는 경우. 이 경우 그 예외의 효력은 3년으로 한다.



선의의 보안 연구(VDP 준수)

CVD 법제화 과제 : 한글 용어 필요

Coordinated Vulnerability Disclosure

보안취약점 협력대응제도

Vulnerability Disclosure Policy

보안취약점 처리 방침

White-hat Hacker

보안연구자

Black-hat vs. White-hat



Source : google

CVD Initiative

It's time to adopt CVD into a cybersecurity framework

보안취약점 협력대응제도 (CVD) 도입

이제, 선택이 아닌 필수

Q & A

감사합니다

Tae Seung Lee

tseung@kisa.or.kr