‘사후대응’에서 ‘사전예방’으로의
정보보안 제도의 ‘패러다임 시프트’를 위한

보안 취약점 신고·조치·공개 제도(CVD/VDP) 도입 로드맵

– 화이트해커와 협력해 보안 취약점을 선제적으로 발굴, 제거 –

2026. 2. 25

국가인공지능전략위원회

보안 취약점 신고·조치·공개 제도 도입 로드맵 (요약)

Ⅰ 추진 배경

□ **초연결 디지털 의존사회·AI시대**, 전통적 **정보보안 체계의 무력化 시작**

○ **AI·클라우드** 기반 초고속 **대규모 사이버 공격 등장과 함께** 파일리스(Fileless) 공격, 공급망 침투 등 기존 **방어우회 신종 위협 확산**

□ 지난 **2025년**은 이러한 **잠재적 위협**이 **현실화** 된 해

○ 침해 사고의 양적 증가뿐 아니라 **대형·중대사고도** 연쇄 발생, **국가행정망**까지 뚫리며 **사이버 위협**의 **안전지대가 '소멸 위기'**에 **직면**

※ (침해사고) '24년 1,887건 → '25년 2,383건(약 26.3% 증가) (KISA) / (대형·중대사고) '25.4 SKT, '25.9 KT, '25.11 쿠팡, / (행정망 해킹) '25.10월 행안부 인정

☞ 기존 정보보안 **체계로는 더 이상 한계, 근본적인 패러다임 변화 필요**

※ (VIP, '25.12.2 국무회의) "**초연결 디지털 사회를 맞이해 민간·공공을 아우르는 '패러다임 시프트' 수준의 새로운 디지털 보안제도** 마련 필요"

Ⅱ 국내 정보보안 제도와 해외 현황

□ **(국내)** 국내 **정보보안 체계는 1회성, 정적점검 위주로 근원적 한계 내재**

○ 정보보안 **인증·점검·평가 등 제도는 年 1회 또는 제품 도입시**에만 실시, **절차점검 위주로** 실시간 **진화**하는 **사이버 위협** 대응에 역부족

※ **(인증)** ISMS, ISMS-P → 年 1회 체크리스트 점검, **(점검)** 보안적합성 검증, 개인정보 영향평가 → 도입시 검증, **(평가)** 개인정보 수준평가, 사이버보안실태 평가 → 절차평가 중심

○ **정보보호 책임자 지정과 관련 공시** 등 제도는 보안 **인력과 투자**의 양을 늘리는 데에는 **기여**하나 **'방어의 질'**은 **보장**하지는 못하는 실정

※ **SKT, KT, LGU+, 쿠팡은 모두 ISMS 인증 획득 및 정보보호 공시·책임자 지정에도 불구 사고 발생**

< 국내 정보보안 제도 현황 >

구분		과기부	개인정보위	국정원
보호 관할		민간 정보통신망 보호	민간·공공 개인정보 보호	국가·공공기관 사이버 보안
운영제도	사전 예방	정보보호공시, 정보보호책임자 지정	개인정보보호책임자 지정, 개인정보영향평가(시스템 도입시)	보안성 검토, 보안적합성 검증(장비 도입시)
	주기적 대응	정보보호인증(年1회), 취약점 신고포상제(年중)	개인정보보호인증(年1회), 개인정보 보호수준 평가(年1회)	사이버보안관리실태평가(年1회), 사이버보안훈련(年1회)
	사고시 제재	2년 이하 징역 또는 2천만원 이하 벌금	전체 매출의 3% 이내 과징금 / 5년 이하 징역 또는 5천만원 이하 벌금	원인분석, 결과통보, 유출 자료 국가안보 영향 평가 등
한계		**실시간** 이루어지고, **상시적으로 고도화**되는 **해킹**에 대한 **방어능력 검증, 대응능력 향상과 동떨어진 상황**		

□ **(해외)** 美·EU는 우리나라와 달리 민간(화이트해커)과 협력, **상시적·선제적**으로 보안 **취약점을 신고·조치**하고 **공개**(CVD/VDP*)하는 **정책** 운영

* **C**oordinated **V**ulnerability **D**isclosure : 조정된 취약점 공개 / **V**ulnerability **D**isclosure **P**olicy : 취약점 공개 정책

[참고] 취약점 신고·조치·공개제도(CVD/VDP) 개요 및 국내 관련 현황

■ **(개요) 기업·기관**이 **자사 정보통신망·제품** 등에 대해 **화이트해커가 취약점을 상시 발굴**할 수 있게 관련 정책을 공개(해킹범위·신고절차 등)하고(=VDP), **화이트해커**는 해당 정책을 준수, **취약점**을 **발굴·신고**하며 기관은 **신고된 취약점을 조치**하고 공개(=CVD)

■ (**국내**) 화이트해커의 **정보통신망 침입 행위**가 선의의 목적이어도 **불법**으로 **간주**(정보통신망법 위반)되어 **제도 미운영** ⇨ **정보통신망이 아닌 제품**(SW) 만을 대상, 취약점을 신고하면 포상하는 **'신고 포상제*'**만 운영(신고 취약점에 대한 **조치 강제력 부재)**

* 과기부·KISA 운영 / 분기별 1회 총 1천만원 수준 포상금(기업이 아닌 정부가 지급)

○ **해당 제도** 운영을 美는 **공공 의무화, 민간**은 공공조달 필수요건 연계 등 **참여** 유인, **EU는 공공 의무화**에 **민간도 상당부문** 의무화*(또는 추진 중)

* [대상] 에너지, 은행, 택배 등 국민 생활 필수·중요 분야 서비스(완료) + 제품 전체(추진 중)

○ **제도도입 배경**에는 **'10~'20년대 세계적 대란 수준**의 보안사고 존재

※ (워너크라이, '17) 美국가안보국이 발견했으나 미공개한 윈도우 취약점이 150개국 해킹 활용 / (솔라윈즈, '20) 취약점 SW업데이트 파일이 美연방기관 연쇄 해킹

- 해당 사태를 계기로 정보보안에 대한 **인식**이 **기존 내부인력 위주 폐쇄적 대응·사후 조치**에서 **개방형 협력·사전 대응**으로 변화

※"우리가 의존하는 기술의 안전보장을 정부 혼자서 해낼 수 없다. 취약점을 식별/수정하기 위해 민간 화이트 해커의 도움이 필요하다."(美 사이버인프라보안국 국장, '21)

☞ 이러한 시대적 상황은 바로 **우리나라가 지난해** 겪은 **보안사태**와 유사

Ⅲ 고려 사항 및 제도 도입 방안

[참고] 국가AI전략위원회 전문가, 관계부처 논의 경과

- **(전문가 논의) 해커원**('25.12.24) ※ 전 세계 최대 화이트해커(240만명 가입) 플랫폼
- **(관계부처 협의) 과기부, 국정원, 개인정보위, 법무부, 조달청** 등 ※ 총 5차례
- **(시민단체 의견수렴) 민변·시민사회·장애인** 인권단체 소속 사회분과 위원('25.12.30)

1 주요 고려 사항

❶ **(인식·평판)** 해당 제도로 취약점이 **공개될** 시 보안 실패로 간주되어 **기업·기관 이미지 실추 우려**, 해커에 대한 부정적 시각도 여전

☞ 참여기업·화이트해커가 **보안향상 우수 기업·기여자**라는 **인식 형성**과 함께 **기업·해커들**에 대한 보호 제도 동반 필요

❷ **(책임 소지)** 정보통신망 침입 이외에도, **취약점 탐색 과정**에서 의도치 않은 **개인정보 확인**, 정보통신망 저해 등 다양한 **책임 소지** 존재

☞ **기업·화이트해커가 책임**질 수 있는 **부문**과 **그렇지 않은 부문**을 명확히 하고, 책임질 수 있는 부문에 대한 **법·제도적 보호장치** 필요

※ (예 : 美 국방부 요구사항) 취약점 탐색 관련 △어떠한 경우에도 데이터 유출 금지, △상업적·재정적 이익 고의침해 방지, △접근권한 없는 정보노출 시 영구삭제 및 국방부 보고

❸ **(역량)** 제도 운영이 **기업·기관의 업무 마비**를 일으킬 **가능성**(전담 인력·예산 부족), 충분한 화이트해커 확보와 관련 역량도 필요

☞ **기관 역량**을 고려해 **단계적**으로 **확대**하고, 제3기관을 활용한 **제도 도입·운영 지원**과 함께 국내 화이트해커 등 **보안 인력 육성 필요**

2 도입 방안

○ **(대상)** 초기에는 **참여 기업·기관 모집**을 통해 시행하되 궁극적으로는 美와 유사하게 **공공**은 **의무화**, **민간**은 **전면적인 참여 유도** 목표

○ **(운영 방식)** 美·EU와 동일하게 대상 기관, 기업이 정한 **정책 범위 내** 화이트 해커에게 **모든 정보통신망·서비스**에 대한 **취약점 탐지** 허용

- **피신고 기업·기관**은 **취약점**을 **조치**하고 조치한 이후, 화이트해커와의 협의를 통해 일정시일 내 **기업·기관명/취약점** 등 공개

- 다만, **기업·기관·화이트해커 실명**은 본인 의사를 고려해 **익명 공개** 허용

- **영세 기업·기관**에 대해서는 KISA 등을 통해 1차 취약점 신고 접수와 선별, 기관 전달 등을 수행하고, **취약점 조치 지원**도 병행*

* AI취약점 자동 분석·검증 플랫폼 구축, API 보급 등 지원 병행

○ **(참여 유인) 공공**은 **기관 평가** 연계, **민간**은 보안인증 가점·**공공조달 우대, 화이트 해커는 신고 포상제 활성화로** 초기 참여 유도

- 특히 **개보법**에 따른 **사고시 과징금**에 해당제도 운영 노력을 **감경**요소로 반영

○ **(보호 장치)** 초기에는 **참여기업·기관-화이트해커 상호 협의**하에 운영하되, 궁극적으로는 관계 **법률 개정**을 통해 **민·형사 처벌 면제 명확화**

○ **(인식 개선)** 화이트 해커와 제도 참여 기업·기관, 정부간 **협력 네트워크** 구축 및 홍보 캠페인, **정부표창 수여 등 인식개선** 추진

Ⅳ 추진 로드맵

□ **(1단계 : 시범사업(~'26)) 민간 분야**는 **과기부, 공공 분야는 국정원** 주도로 **시범 사업**을 운영, 국내 제도 도입 가능성과 효과를 사전 검증

※ (예) 5~10개 선도기관(기업/공공기관)과 KISA, 화이트해커 등 참여, 해당 제도 실효성을 현실 환경에서 검증, 규제샌드박스 제도 연계로 최대한 美·EU와 유사한 환경 조성

□ **(2단계 : 참여 확대(~'27)) 시범사업 바탕 민간**(과기부)·**공공**(국정원) **분야 제도 설계 및 관련 가이드라인 마련·배포, 관계부처 참여유인 제공**

□ **(3단계 : 법제화(2단계 상황 고려, 최대한 조속히 추진)) 관계 법령 개정 완료**

※ (정비검토 대상) 정보통신망법(과기부/법무부), 개인정보보호법(개보위), 국가정보보안 기본지침(국정원), 저작권법 지침(문체부), 기타 민·형사 리스크방지 지원(법무부)

Ⅴ 향후 계획

□ **민간(과기부)·공공(국정원) CVD/VDP 시범 사업 시행** : '26.하반기

목 차

Ⅰ. 추진 배경 1

Ⅱ. 국내·외 현황 2

1. 국내 정보보호 제도 현황 및 한계 2

2. 해외 취약점 신고·조치·공개 제도 운영 현황 ·· 7

Ⅲ. CVD·VDP 제도 도입방안(안) 14

1. 사전 고려 사항 14

2. 도입 방안(안) 15

Ⅳ. 추진 로드맵(안) 17

Ⅴ. 향후 계획 18

※ [붙임] 대한민국 AI행동계획(안) 관련 문구 19

Ⅰ. 추진 배경

□ 초연결 디지털 의존 사회 → 단일 보안 사고가 대규모 피해로 직결

○ 우리나라는 세계적으로 앞선 디지털 인프라를 구축 중이나 동시에 **단일 보안사고**가 **대형재난**으로 **비화**될 수 있는 구조적 취약성 내포

○ 아울러 **초개인화 서비스의 보편化는** 신상정보를 넘어 생활패턴·취향 등 민감 정보까지 유출될 수 있는 **대형 리스크를** 함께 **수반**

□ AI·클라우드 기반 신종공격 확산 → 공격자에게 기울어진 운동장

○ AI 확산과 함께 AI로 취약점을 자동 스캔하고 공격 코드를 생성하는 초고속 대규모 사이버 공격 등장, **해킹의 기법이** 날로 **진화**

- **공격자**가 **수만개**의 시스템을 수십분만에 장악하는데 비해 **방어자**는 **단일 사고 대응**에만 수십일이 소요, '**공수(攻守)의 비대칭**' 심화

○ 또한 파일리스(Fileless) 공격, 공급망 침투 등 **기존 경계 기반 방어**를 우회하는 **신종 위협 일상化**, 전통적 보안체계의 '**무력化**' 시작

□ '25년 대형사고 연쇄 발생 → 구조·제도적 취약성 현실化

○ '25년은 이러한 **잠재적 위협이 현실화** 된 해, 사고의 양적 증가*뿐 아니라, **대형·중대사고**도 연쇄 발생(4월 SKT, 9월 KT, 10월 LGU+(신고접수), 11월 쿠팡 등)

* (침해사고 건수) '24년 1,887건 → '25년 2,383건(약 26.3% 증가) (KISA)

○ 특히, **민간 기업**뿐 아니라 **국가 안보**의 보루인 행정망(행안부 인정, '25.10월)까지 뚫리는 등 **사이버 위협**의 **안전 지대가 소멸 위기에 직면**

☞ **초연결·AI시대** 기존의 **정보보안 체계**로는 **더 이상 한계 도달**

→ **사고발생** 후 **조치 중심** 패러다임을 극복, **위협**을 선제적으로 **찾고 미리 제거**하는 **능동적이고 상시**적인 **예방 체계**로 **大전환** 필요

※ (VIP, '25.12.2 국무회의) "**초연결 디지털 사회를 맞이해 민간·공공을 아우르는 '패러다임 시프트' 수준의 새로운 디지털 보안제도** 마련 필요"

Ⅱ. 국내·외 현황

1 국내 정보보호 제도 현황과 한계

◇ 우리나라는 **과학기술정보통신부, 개인정보보호위원회, 국가정보원** 등 **부처별 역할 분담**을 통해 **민간 공공의 정보보호 제도를 운영** 중이나,

☞ **'1회성 진입규제', '정적점검', '폐쇄적·사후처벌'** 중심으로 해당 제도만으로는 **'상시·지능적'**으로 진화하는 **최신 사이버 위협 대응에 근원적 한계**

□ 과기정통부 : 민간 부문 정보통신 분야 보안 총괄

○ **민간 기업**의 정보보호 인증, 정보보호 공시 및 책임자 지정 등 기반 조성과 취약점 신고 포상 등 제도 운영으로 **자율 대응역량 제고**

❶ **(ISMS* 인증) 기업의 정보보호 정책·조직·기술 보호조치** 등을 주기적(年1회)으로 평가, **일정수준 이상 관리**를 유도

* 정보보호 관리 체계(Information Security Management System)

☞ **기업의 정보보호** 체계 조성에 **기여** 중이나 **프로세스** 위주 평가로 실제 운영 서비스의 실시간 **취약점 탐지·방어능력 검증 한계**

❷ **(정보보호 공시·책임자)** 민간 기업의 **보안 투자 유도**를 위해 정보보호 투자액·인력 현황 공개와 **정보보호책임자**(CISO) **지정**을 의무화

* Chief Information Security Officer : 정보보호 최고책임자

☞ 정보보호 **예산과 인력**의 양을 늘리는 데에는 기여하고 있으나, **실제 공격**을 보호하는 **'방어의 질'**을 보장하지는 않는 상황

※ KT, LGU+, 쿠팡은 모두 ISMS 인증 획득. 정보보호공시, CISO 지정 기업임에도 사고 발생

❸ **(취약점 신고 포상제)** 분기별로 민간 기업의 취약점을 신고하는 국민에게 **포상금**(최대 1천만원) **지급하는 제도 운영**

☞ **현행법은 취약점 제보를 위한 망 접근**을 불법 침입으로 간주*, 망이 아닌 **제품위주 제한적 신고****, 발굴 취약점 **조치 강제력도 없음**

* 정보통신망법 제48조(정보통신망 침해행위 등의 금지)

** ① **제품위주** 발견 → ② 기업 전달(**조치 강제력 없음**) → ③ 기업이 아닌 정부 포상

□ 개인정보위 : 민간·공공 부문 개인정보 분야 보호정책 수립·운영

○ **공공/민간의** 이원화된 **제도** 운영으로 **개인정보 보호 역량 제고**

❶ **(공공부문 개인정보 보호수준·영향평가)** 공공기관의 **개인정보 관리 체계** 年 1회 평가, 개인정보처리 **시스템 구축 시** 사전 **위험요인** 분석 등

❷ **(민간·공공 책임자 지정, 민간 ISMS-P 인증*)** 개인정보보호책임자(CPO) 지정 의무화, 개인정보보호 관리체계 인증 유도

* 정보보호 및 개인정보보호 관리 체계(Personal Information & Information Security Management System)

❸ **(민간 사후 제재)** 사고발생 시 **전체 매출의 3% 이내 과징금 부과** 등

☞ 평가/인증 등 제도는 1회성에 **체크리스트·문서 등 행정 중심**의 정적 점검으로 민간, 공공의 상시대응 능력 확보에 한계

☞ 과징금 부과는 기업의 정보보호 **경각심 제고**에 **기여** 중이나, 평상시 노력을 고려한 경감* 등 **상시적 노력 유인**에는 미흡

* **상시 노력을 평가할 수단 부족으로 사전 인증, 사후 대처 등을 중심으로 과징금 산정 반영**

□ 국정원 : 공공 부문 사이버 보안 분야 총괄

○ **국가·공공기관**의 **정보(사이버) 보안 정책**을 총괄 수립·감독, 시행

❶ **(보안 적합성 검증·보안성 검토) 국가·공공기관**의 정보화 사업, 정보보호시스템/네트워크 장비 도입·구축시 **사전 적합성·보안성 검증**

❷ **(사이버 보안 실태 평가) 매년 전 공공기관** 대상 **사이버 위협에** 대한 **대응 역량을 평가**(현장실사 등)하여 대상 기관의 경영평가에 반영

❸ **(사이버 정보 공유, 사이버 위기 대응 훈련)** 국제·국가배후 해킹조직 등 사이버안보 관련 정보 수집·배포·공유, 年 **1회 대응훈련** 시행

☞ **적합성·보안성 검증**은 도입 시스템의 보안 향상에 기여 중이나, 지능화되는 해킹기법 대응, 운영단계 발생 **신규 취약점 추적관리**에는 **한계**

☞ 단순 정보 공유, **시나리오 기반 사이버 대응훈련**은 **실시간으로 고도화**되는 **해킹공격**에 대한 각 기관 실전의 **방어능력 향상**에는 역부족

참고 우리나라 정보보안 체계, 관련 제도 현황 및 한계

□ 전체 제도 개요

구분		과기정통부	개인정보위	국정원
관할		민간 정보통신망 보호	민간·공공 개인정보 보호	국가·공공기관 사이버 보안
운영제도	사전 예방	정보보호 공시 + 정보보호책임자 지정(CISO)	(공공) 개인정보 영향평가 + (민간·공공) 개인정보보호책임자 지정(CPO)	보안적합성 검증 + 보안성검토
	주기 대응	정보보호인증 (ISMS) (年1회) + 취약점 신고포상제(상시)	개인정보보호인증 (ISMS-P) (年1회) + 개인정보 보호수준 평가 (年1회)	사이버보안 관리실태 평가 (年1회) + 사이버보안 훈련 + 위협정보 공유 (상시)
	사고 발생 시 제재	자료보전 명령을 위반한 정보통신서비스 제공자(기업 등)에게 2년 이하의 징역 또는 2천만원 이하의 벌금 부과 ※ 침해사고 발생 자체에 대한 처벌규정은 부재	개인정보처리자(기업·기관)에 전체 매출의 3% 이내 과징금 + 개인정보처리자(기업·기관) 5년 이하 징역 또는 5천만원 이하 벌금 부과	사이버공격 주체 규명, 원인 분석 및 결과 통보 + 유출 자료 국가안보 영향 평가
한계		**실시간 이루어지고, 상시적으로 고도화되는 해킹에 대한 방어능력 검증, 대응능력 향상과 다소 동떨어진 상황**		

□ [과기부-개보위] ISMS/ISMS-P 인증제도 ※ '18년부터 통합운영 중

<table>
<tr><th>구분</th><th>(과기부) ISMS</th><th>(개보위) ISMS-P</th></tr>
<tr><td>법적 근거</td><td>정보통신망법 제47조(정보보호 관리체계 인증)</td><td>정보통신망법 : 좌동
+
개인정보보호법 제32조의2
(개인정보보호인증)</td></tr>
<tr><td>인증 기관</td><td colspan="2">KISA 또는 과기부·개보위 지정 인증기관</td></tr>
<tr><td>의무 대상 기관</td><td>정보통신망서비스 제공자,
정보통신서비스 제공자 중 전년도 매출 100억원 이상 또는 일일평균 이용자 100만명 이상 등*
* 이外 상급종합병원, 학교 일부 포함</td><td rowspan="2">해당없음

(민간 자율)</td></tr>
<tr><td>벌칙</td><td>의무대상자 미이행시 3천만원 이하 과태료 부과(정보통신망법 제76조)</td></tr>
<tr><td>방식 / 효력</td><td colspan="2">최초 심사 후 2년간 사후 심사, 3년이후 갱신심사 운영
※ 최초(1년)–사후(1년)–사후(1년) -갱신(1년) /
최초심사 후 사후심사에서 특이사항 없을시 3년간 효력 유지</td></tr>
<tr><td>점검 리스트</td><td colspan="2">
<table>
<tr><th rowspan="2">인증 영역</th><th rowspan="2">인증기준(갯수)</th><th colspan="2">적용 영역</th></tr>
<tr><th>정보보호 (ISMS)</th><th>개인정보보호 (ISMS-P)</th></tr>
<tr><td>1. 관리체계 수립 및 운영</td><td>관리체계 기반 마련, 위험관리, 관리체계 운영·점검·개선 등(16개)</td><td>○</td><td>○</td></tr>
<tr><td>2. 보호대책 요구사항</td><td>정책·조직·자산, 인적·외부적·물리 보안, 인증·권한관리, 통제·암호화, 정보시스템 도입·개발보안, 시스템·서비스 운영관리, 사고 예방 및 대응, 재해복구 등(64개)</td><td>○</td><td>○</td></tr>
<tr><td>3. 개인정보 처리단계별 요구사항</td><td>개인정보 수집, 보호 및 이용, 제공, 파기시 보호조치, 정보주체 권리 보호 등 (21개)</td><td>X</td><td>○</td></tr>
<tr><td colspan="2">항목수 합계</td><td>80개</td><td>101개</td></tr>
</table>
</td></tr>
<tr><td>한계</td><td colspan="2"><u>1년에 한번 체크리스트 위주 점검 수준</u></td></tr>
</table>

□ [개보위] 개인정보 영향평가 / [국정원] 보안적합성 검증

구분	(개보위) 개인정보 영향평가	(국정원) 보안적합성 검증
법적 근거	개인정보보호법 제33조 (개인정보 영향평가)	국가정보원법 제4조(직무) / 전자정부법 제56조(정보통신망 보안대책)
평가 주체 /대상	개인정보보호위원회 지정 기관 / 공공기관 도입 일정 규모 이상 개인정보 파일을 구축·운영체계	국가정보원 / 국가·공공기관 도입 정보보호 시스템·네트워크 장비 및 양자암호통신장비
방식 / 주기	평가대상 체계 구축·운용시 평가기관 평가를 거쳐 개인정보 침해 우려 사항 조치 이후 운용 ※ 체계변경시 재신청	검증대상 제품도입 시 국정원 신청·검증을 거쳐 취약점 제거 등 보안 조치 이후 장비 운용 ※ 제품형상 변경시 재신청
미이행 벌칙	미수행 시 3천만원 이하 과태료	법령상 별도 명시는 없으나, 기관 평가 등에서 간접 반영
한계	**시스템 도입·변경 시 1회성 평가·검증**	

□ [개보위] 개인정보 보호수준 평가 / [국정원] 사이버보안 실태 평가

구분	(개보위) 개인정보 보호수준 평가	(국정원) 사이버 보안 실태 평가
법적 근거	개인정보보호법 제11조의2 (개인정보 수준평가)	국가정보원법 제4조(직무) ※ 세부 : 국가정보보안 기본지침
평가 주체 /대상	개인정보보호위원회/ 중앙행정기관 및 소속기관	국가정보원 / 중앙행정기관 및 소속기관
방식 / 주기	정량(자체평가) + 정성지표(개보위 평가) 평가/ 年 1회	기관자체평가 + 국정원 현장점검 / 年 1회
평가 반영	자료 미 제출 시 1천만원 이하 과태료 부과, 미흡 기관 개선권고, 우수기관 포상, 정부업무평가 반영 등	정부업무평가에 반영 등
한계	**정해진 체크리스트 중심 규정 준수/시나리오 대응 중심**	

2 해외 취약점 신고 조치·공개 제도 운영 현황

◇ **美·EU**는 우리나라와 달리 **민간**(화이트해커)과 **협력**하여 **상시 취약점**을 **발굴·제거**하고 공개하는 **개방형 협력 정책을 국가차원의 정보보호 전략**으로 활용

1. 개 요

□ 취약점 신고·조치·공개제도(CVD·VDP)

※ **[용어] CVD**(Coordinated Vulnerability Disclosure) **: 취약점 신고·조치·공개 프로세스 / VDP**(Vulnerability Disclosure Policy) **: 취약점 신고·조치·공개 정책**

○ (CVD) **화이트해커**가 발견한 **취약점**에 대해 기관이 **신고 접수, 조치,** 외부에 **공개**하는 취약점 관리 프로세스(발굴→신고→조치→공개(조율))

※ 아울러 **화이트해커의 CVD/VDP 참여**를 위해 **취약점**(Bug) **발견자**에게 **포상금**(Bounty)을 지급하는 '버그바운티' 제도도 자율적 운영 연계

○ (VDP) 기업·기관이 해킹범위·신고절차·공개시기 등을 명시하고 이를 외부에 공개하여 **화이트해커가 CVD를** 할 수 있도록 하는 정책

- **해당 정책을 준수하는 범위** 내에서 화이트해커는 상시적으로 기업·기관의 망·제품을 해킹하여 취약점을 발견, 신고 가능

기업·기관	⇨	화이트해커	⇨	기업·기관, 화이트해커
VDP 운영		VDP 준수, 취약점 탐색·신고		CVD 의거, 접수조치, 공개(화이트해커와 시기/방식 조율)

□ 해외 도입 배경 : 대규모 보안사고 → 정보보호 인식 전환

○ 美, EU 역시 **2020년대** 이전까지는 **우리나라와 유사**하게 '진입 시 일회성 검증', '폐쇄적 보안'만을 **정보보호 정책의 핵심 축**으로 운영

- **(진입 인증)** CC 인증*, CE** 인증 등 **새로운 해킹 기법**이 나와도 한번 통과하면 수년간 **효력**(3~5년)**이 유지되는 제도** 운영

* CC(Common Criteria) : 정보보호 제품의 보안성을 평가하는 국제 표준(ISO 15408)
** CE(Conformité Européenne) EU내 제품 판매에 필수적인 적합성 안전 마크

- **(폐쇄적 보안)** 美·EU는 **망 보호 기여를 위한** 외부의 **선의적 접근까지 포괄적**으로 **차단·처벌**하고, **내부인력** 또는 외부 **소수 전문가**에 의존

※ 컴퓨터 사기 및 남용 방지법(美), 사이버범죄 협약(EU) 등에 따라 외부 전문가의 선의의 취약점 탐색 행위뿐 아니라, 모의해킹 도구 제작·배포까지 범죄시 처벌

○ **디지털 확산과** 함께 **2010 ~ 2020년대 대형 보안사고**가 연쇄적으로 발생하며, 정보보호 정책을 바라보는 **시각**의 **대전환** 시작

- **(사고)** 워너크라이(WannaCry, '17)* 솔라윈즈(SolarWinds, '20)** 등 발견 후 **은폐되거나 또는 방치되고 있던 취약점들이 세계적 대란 초래**

* 美국가안보국이 발견하였으나 미공개한 윈도우 취약점이 해킹에 활용되 전 세계 150개국 감염 / ** SW 업데이트 파일 설치 美국무부·재무부 등 연방기관 연쇄 해킹

- **(정책) 내부 인력, 폐쇄적 정책**만으로는 더 이상 **모든 취약점 방어**의 **한계, 화이트해커**의 선의적 활용 **필요성**에 대한 인식 확산

※"우리가 의존하는 기술의 안전보장을 정부 혼자서 해낼 수 없다. 취약점을 식별/수정하기 위해 민간 화이트 해커의 도움이 필요하다."(美 사이버인프라보안국 국장, '21)

☞ 현재 **우리나라와 유사한 환경**에서 **美, EU가 기존 제도의 한계를 극복**하기 위해 채택한 정책이 바로 **취약점 신고·조치·공개제도(CVD·VDP)**

2. 美, EU 도입 현황

□ 미국 : 공공 도입 의무, 민간 도입 강력 권장

○ **(공공)** CVD・VDP 제도 **도입 의무화**, 이행을 강제

- **(제도) 사이버·인프라보안국***이 **연방정부 행정기관**에 인터넷 접속 가능 서비스·제품에 대한 **CVD・VDP 의무 도입**** 지시, 각 기관 이행

* (CISA : Cybersecurity and Infrastructure Security Agency) 미국 국토안보부 산하 공공·민간 보안전담 기관(우리나라 과기부의 국정원 보안기능 병행)

** 연방정보보안현대화법(FISMA)에 근거한 구속력 있는 보안 지침 BOD 20-01 조항 근거

- **(이행력 확보)** 미준수 시, **사이버인프라·보안국이 해당기관**에 시정 명령 발동, 백악관 관리예산국(OMB), 의회 보고로 행정·재정 불이익 부여

* OMB는 기관 예산편성·성과 평가 반영, 의회는 청문회 개최로 기관장 소환 등

○ **(민간) 민간자율**이나 공공조달·사고시 **처벌 연계**로 **강력 유도**

- **(공공 조달) IoT법***, **OMB, 연방 조달청**은 CVD·VDP 포함 **보안표준****을 **조달계약**의 **필수 요건**으로 설정, 미준수 제품·서비스 **공공 납품 불가**

* IoT Cybersecurity Improvement Act of 2020

** NIST(National Institute of Standards and Technology : 국립표준보안연구소) SP 800-218

- **(처벌 연계)** 美 연방거래위원회는 해킹사고 조사 시 **VDP 운영여부**를 **과징금 등 제재*에 반영, 美법원 역시 소송 시 VDP 운영여부 참작****

* FTC법 제5조 근거, 기업의 VDP 운영 여부를 '합리적 보안 조치'를 수행했는지 판단하는 핵심 근거로 채택, 제재 수위 결정에 반영

** (사례) 오하이오 주는 VDP 성실준수 기업이 해킹으로 집단소송 시 적극항변권 부여

○ **(화이트 해커) 선의의 화이트해커 활동 기소 제외** 선언('22, 美 법무부), 민간 공공의 자발적인 **버그바운티 제도 활성화*로 참여유인** 제공

* (예 : 보상금) 구글 수십만 달러(약 1.5억원~15억) 애플 아이폰 200만 달러(약 30억)

□ EU 현황 : 공공 도입 의무, 민간 부문도 대다수 의무

○ **(공공)** 美와 마찬가지로 **CVD·VDP 도입 의무화, 이행 강제**

- **EU 네트워크 정보보안 지침***을 통해 EU 회원국들로 하여금 **공공기관** 관련 **제도 도입 및** 미준수 시 **기관장 제재** 등 패널티 명문화

* Network and Information Security Directive(NIS2, 네트워크 및 정보 보안 지침)
(이에 따라 현재 기준 EU 회원국 27개국 중 14개국이 해당 제도 도입 중(EU ENISA)

○ **(민간) 제품**과 **서비스**를 구분지어 운영하나, **상당 부문 의무화**

- **서비스**는 **에너지·운송, 우편·택배** 등 **국민생활 필수·중요분야** 의무화(NIS2 지침), **제품**은 제조사·수입사·유통사 대상으로 '27년 전체 의무화 예정*, 미 **이행시**에는 **과징금 부여**(참고1, p10)

* 사이버복원력법(CRA, Cyber Resilience Act : '24년 제정, '27년 시행 예정)

○ **(화이트해커) 윤리적 해커**에 대한 법적 보호 도입 의무화*(EU NIS2), 美와 마찬가지로 민간 공공의 자발적인 **버그바운티 제도 활성화***

* NIS2 내용 中 : **회원국은 화이트해커가 처벌 두려움 없이 취약점을 신고할 수 있게 해야 함**

** (예 : 버그바운티 민간 플랫폼 ntigriti) 누적 포상금 5,000만달러('16~'24.2Q, 약 740억원), 참여기업 400개 이상('24)

☞ **美·EU는 '20년대 대규모 디지털 재난 사태** 이후 **공공/민간 전반**에 **CVD·VDP 제도**를 도입, **상시적**인 **취약점 발굴·조치로 해킹사고**를 방지*

* 美국방부, 테슬라 등 CVD·VDP 활용 취약점 선제 발굴로 대규모 사고 방지(참고3)

→ **우리나라도 이를 벤치마킹**하여 현재의 **국가적 보안 위협사태 극복** 필요

참고1 국내·외 CVD·VDP 제도 운영 현황

<table>
<tr><th rowspan="2">구분</th><th colspan="2">민간</th><th>공공</th></tr>
<tr><th>서비스</th><th>제품</th><th>서비스/제품</th></tr>
<tr><td>미국</td><td colspan="2">민간 자율이나 공공 조달 필수요건, 처벌 연계 등 강력한 유인
- (조달) 연방기관 납품 시 NIST 보안 표준 준수 보안서약서 제출이 필수, <u>VDP는 NIST 표준 (NIST SP 800-218)에 포함</u>
- (행정규제) FTC(연방거래위원회)가 해킹사고 조사 시 VDP 여부에 따라, 과징금 감면, 보안 관리감독, 제3자 외부 보안 감사 의무 등 고려
- (소송) 법적소송 시 합리적 수준 보안 노력의 정상참작 사유(배상액 최소화 등)로 VDP 도입 여부 고려</td><td>민간 자율이나 공공 조달시 필수요건, 처벌 연계 등 강력한 유인
※ 다만 의료기기는 의무(의료기기 제조사는 FDA 인허가 시 CVD 계획 필수요구
- (조달) 좌동, IoT법 (IoT Cybersecurity Improvement Act of 2020)</td><td>연방기관 강제 의무
- (제도) 연방정보보안현대화법 근거(FISMA), 사이버·인프라 보안국(CISA)은 연방기관에 구속력 있는 운영지침(BOD) 발행, VDP는 BOD 20-01('20)에서 연방기관 의무화
* Binding Operational Directive
- (이행력) BOD 미준수 시 공공기관은 강제시정명령, 백악관 관리예산국(OMB) 예산 배분 시 영향, 국회 청문회 출석 등 패널티</td></tr>
<tr><td>유럽</td><td>필수*, 중요**분야 의무
* (필수) 에너지, 운송, 은행, 금융시장인프라, 건강, 먹는물, 폐수, 디지털인프라, 우주 등
** (중요) 우편/택배, 화학물질 제조/생산/유통, 식품 생산/가공/유통, 디지털 제공자 등
※ 네트워크·정보시스템 사이버보안 지침(NIS2)('22)
- (필수) 미준수 시 과징금(1,000만유로, 약 170억원) 혹은 전세계 연매출 2% 중 더 높은 금액), 경영진 제재(직무정지 및 법적책임), 인증/허가정지 등
- (중요) 미준수 시 과징금(700만유로, 약120억원) 혹은 전세계 연매출 1.4% 중 더 높은 금액), 경영진 제재(법적책임) 등 패털</td><td>전체 의무 예정
※ 사이버복원력법(CRA, '24.12월 발효 '27년.12월 시행 예정)
- 미준수 시 과징금 (1,500만유로, 약 255억원) 혹은 전세계 연매출 2.5% 중 더 높은 금액), EU 판매금지, 시장철수, 제품 회수, 공공조달 참여 불가
※ 사이버복원력법(CRA)('24) 시행예정인 '27년부터</td><td>전체 의무
- 미준수 시 기관장 제재(직무정지 및 법적책임), 시정명령, 사전감독(불시점검, 감사) 등 패널티
※ 네트워크·정보시스템 사이버보안 지침(NIS2)('22)</td></tr>
<tr><td>한국</td><td colspan="3"><u>우리나라는 공공/민간 전분야에 CVD·VDP 제도 미운영</u></td></tr>
</table>

참고2 해외 공공·민간 CVD·VDP 제도 실제 운영 사례

□ 국방부 사례

※ 홈페이지 공개

o 점검범위

- **인터넷에 연결된 모든 국방부 소유 정보시스템, 웹사이트, 어플리케이션**

※ (예외) 국방부 내부망, 기밀 시스템, 제3자 운영 시스템 중 국방부 자산 아닌 것

o 신고방법

- **상시적 취약점 접수 사이트인 해커원 플랫폼 통해 취약점** 상세 요약본 제출

※ (제출내용) 취약점이 포함 된 제품명, 버전, SW 구성, 문제를 재현하는 단계별 지침, 개념증명(PoC), 문제 영향, 적절한 수정 조치 제안 등

o 가이드라인(제한사항) 일부

- 원격 수단을 통한 취약점 탐지 또는 테스트
- **취약점, 취약점 관련 지표에 대해 국방부와 단독 공유**, 국방부로부터 정보 수신
- 취약점을 입증하거나 취약점 관련 지표를 식별하는데 필요한 최소한의 테스트의 범위를 초과하여 **취약점을 악용하지 못함**
- 어떤 상황에서도 **데이터 유출 금지**
- 국방부 직원 또는 기관, **제3자의 지식재산권, 상업적·재정적 이익을 고의로 침해하지 않을 것**
- **국방부 서면 허가 받지 않는** 취약점의 세부사항, 취약점 지표, 취약점으로 인해 노출된 정보 내용을 **공개적으로 공개 불가**
- **취약점 확인 중 일반인의 접근 권한이 없는 정보에 노출된 경우 국방부의 지시**에 따라 보유 중인 **모든 확인된 정보를 영구적으로 삭제하고 이를 국방부에 보고**

o 취약점 공개시기

- **국방부는 1일 내 보고서 접수승인/ 취약점 공개는 국방부의 명시적 서면동의 이후**

o 법적면책 조항 : VDP 프로그램의 조건에 따라 일하는 보안 연구원이 취약점을 공개할 경우, 국방부는 권한 행사 시 다음과 같은 조치를 취합니다

(1) 해당 연구자에 대해 그러한 활동과 관련된 **어떠한 법 집행 조치나 민사 소송도 개시하거나 권고하지 않으며,**

(2) **법 집행 기관 또는 민사 원고에게 연구자의 활동이** 프로그램의 조건을 준수하여 진행되었음을 알립니다.

※ **VDP 프로그램을 준수하지 않으면 보안 연구 활동과 관련하여 모든 관련 연방, 주 및 지방 법률을 준수**해야 합니다. 프로그램 또는 법률의 약관과 일치하지 않는 보안 연구 또는 취약점 공개 활동은 할 수 없습니다. 프로그램 조건이나 법률에 부합하지 않는 활동을 할 경우, 보안 연구원으로 간주되지 않으며 형사 처벌 및 민사 책임을 질 수 있습니다.

□ Microsoft MS 사례

※ 홈페이지 공개

O 점검범위

- 마이크로소프트 제품이나 서비스 및 여기에 포함 된 서드파티 및 오픈소스 구성요소

※ (제외) 데이터조작, 네트워크 접근, MS 사무실 혹은 데이터센터 공격, 직원에 대한 사회공학 공격 등

O 신고방법

- **CVD 절차에 따라 마이크로소프트 사이트를 통해 취약점** 상세 내용 제출

※ (제출내용) 문제 유형(SQL 인젝션 등), 제품 버전(온라인서비스는 URL), 버그 설명, 문제를 재현하는 단계별 안내(필요 시 문제를 재현하기 위한 특수구성 포함), 개념증명(PoC), 공격자 악용에 대한 영향 등

O 가이드라인(제한사항) 일부

- 미국 제재를 받고 있는 국가 또는 프로그램 참여를 허용하지 않거나 MS 수출 정책에 의해 금지된 국가의 거주자 및 14세 미만 제한
- 불법적인 행위 금지
- 바이러스 전파, 테러 콘텐츠 게시, 증오발언 등 본인, 프로그램, 타인에 해로운 활동 금지
- 타인의 권리 침해 금지 등
- 귀하에게 적용되는 모든 법률을 준수해야 하며, 버그 보상 프로그램이 허용하는 범위를 넘어 데이터를 방해하거나 유해 금지
- 취약점 보고 제출물을 **비밀로 유지**할 것을 요구하며, 제3자나 논문리뷰, 학회 제출 일부로 공개 될 수 없으며, 취약점 수정된 이후에는 연구에 대한 설명과 시연 제공 가능

O 취약점 공개시기

- **MS는 영업일 1일 내 보고서 접수/ 취약점 공개는 수정 이후 가능**

O 법적면책 조항

- **보안 취약점에 대한 연구와 책임 있는 공개를 장려**하기 위해, **Microsoft Bug Bounty 이용 약관("정책")의 우발적 또는 선의의 위반에 대해 민사 또는 형사 소행을 추구하거나 법 집행기관에 통지를 보내지 않을 것**이며, 이 정책에 따라 수행되는 **보안 연구 및 취약점 공개 활동**을 컴퓨터 사기 및 남용방지법(DMCA), 그리고 워싱턴 형법 9A.90과 같은 기타 적용 컴퓨터 사용 법률에 따른 **"승인된" 행위로 간주**함. 버그 바운티 프로그램 범위 내 애플리케이션을 보호하기 위해 사용한 기술적 조치를 우회한 것에 대해 발생할 수 있는 **저작권법(DMCA) 청구를 포기**
- 화이트해커의 취약점 연구가 **제3자**(제3자의 네트워크, 시스템, 정보, 애플리케이션, 제품 또는 서비스)와 관련된 경우, 제3자를 구속할 수 없어, 제3자가 법적 조치나 법 집행 통지를 할 수 있음.
- 타 기관의 이름으로 보안 연구를 승인할 수 없으며, 귀하의 행위에 근거한 제3자 행위로부터 방어, 면책 또는 보호를 제공할 수 없음

참고3 국내외 CVD · VDP 제도 운영 효과

□ 해외 기관 · 기업 VDP/CVD 주요 성과 사례

기관명	사례
美 국방부 (DOD)	o **(사례)** 美 국방부는 '16년 「Hack the Pentagon」에서 **24일**만에 화이트해커 1,410명이 **유효한 138개 보안 취약점**(총 1,189건) **발견에 7.5만달러**(약 1.1억원) 소요 o **(효과)** 기존 외부 보안업체에서 진행하던 보안감사 비용은 **100만달러(약 15억원) 이상**이나, **더 적은 비용으로 해결**(美 국방부 장관 애쉬카터('16.6)
shopify 쇼피파이	o **(사례)** 쇼피파이는 '16년 **관리자페이지에 개인정보**(이름, 주소 등)가 포함되어 있었으나 **VDP 기반 취약점 신고로 당일 패치**하여 **개인정보 유출 되지 않음** o **(효과) 30만명**의 상점 데이터 **유출 사고 위험으로, 만약 사고시** 美 정부합의금(FTC 등), 집단소송, 사고수습 비용 등 **약 700억원의 지출 가능성이** 있었으나 **1,000달러(약 140만원)의 포상금만 지급**(2025 IBM 보고서)
TESLA 테슬라	o **(사례)** 테슬라는 '16년 텐센트 킨 보안연구소가 **테슬라 VDP에 따라 주행 중인 자동차를 원격으로 해킹**해 브레이크 제어 등의 취약점을 발견하여 신고하였고 **테슬라측은 무선을 통해 모든 차량 보안 패치** o **(효과) 해커 발견 시 전량 리콜 가능성, 약 240억원의 리콜 지출* 대신 40,000달러(약 5,900만원)의 포상금만 지급해** 해결 * 2016년 당시 테슬라 출고 약 16만대 기준, 리콜 대당 약 $100 비용 발생 적용 계상

□ 취약점 조치 통계

구분	주요내용
美 국방부	**'16년~'24년까지 CVD·VDP** 제도를 통해 총 누적 **취약점 5.4만건 처리**, '22년까지 처리된 취약점 중 **약 3,500건**은 시스템이나 네트워크에 심각한 피해(서비스 중단 등)를 줄 수 있는 **고위험 등급 결함 판명** ※ (출처) 미 국방부 사이버 범죄센터 연간 리포트
[참고] 우리나라 (과기정통부) 취약점 신고포상제	'25년 1~12월까지 신고받은 취약점은 **2,525건**으로, 해당 기업에게 신고받은 취약점 정보를 전달·조치 요청. 포상은 781건, **취약점 공개 건수는 3건 수준** * '20년 71건 → '22년 12건 → '24년 7건 → '25년 3건 (KISA)

Ⅲ. CVD · VDP 제도 도입 방안(안)

1 사전 고려사항

1 사회적 인식 · 평판

○ (기업/기관) CVD·VDP 제도로 취약점이 발굴·공개될 시, 이를 '**보안 실패**'로 간주, 참여 기업·**기관의 이미지 실추**, 주가 하락 등 우려

○ **(화이트해커) 해킹에** 대한 사회적 **부정적 시각**과 자신의 취약점 발굴 노력이 **기업 성과**로만 **포장**될 가능성에 대한 우려

☞ 참여 기업/화이트해커가 보안 향상 우수 기업/기여자라는 **인식 형성**과 함께 필요시 기업/해커 **익명성** 보장, **인센티브 정책** 등 필요

2 책임 소지

○ **(기업·기관)** 진단 과정에서 서비스 장애나 개인정보 유출사고 책임, **취약점 점검 허용을 악용**한 데이터 탈취·백도어 설치 등 연결 불안감

○ **(화이트해커)** 망 침입 이외에도, **취약점 탐색 활동 과정**에서 의도치 않은 **개인정보 확인**, 망 저해 등 다양한 **책임 소지** 존재

☞ **기업·화이트해커가 책임**질 수 있는 **부문**과 **그렇지 않은 부문**을 **명확화**하고 책임질 수 있는 부문에 대한 **법·제도적 보호장치** 필요

※ (예 : 美 국방부 요구사항) 취약점 탐색 관련 △ 어떠한 경우에도 데이터 유출 금지, △ 상업적·재정적 이익 고의침해 방지, △ 접근권한 없는 정보노출 시 영구삭제 및 국방부 보고

3 기관 · 인력 역량

○ 제도 운영이 **기업·기관의 업무 마비**를 일으킬 **가능성**(전담 인력·예산 부족), 아울러 충분한 화이트해커 확보 및 관련 **역량**도 필요

☞ **기관 역량**을 고려한 **순차 적용** 확대, 제3기관을 활용한 **제도 도입·운영 지원**과 함께 국내 화이트해커 등 **보안 인력 육성 병행** 필요

2 도입 방안(안)

◇ 현재 과기부가 운영 중인 **취약점 신고 포상제 제도**를 전면 개편, **美와 유사**하게 **공공 단계적 제도화(의무), 민간 도입촉진 방식 VDP/CVD 제도 도입 제언**

구분		취약점 신고포상제		취약점 신고·조치·공개제도(CVD·VDP)
1 대상	공공	-		**단계적 제도화(의무) 목표**
	민간	민간기업		**전체 참여 유도**
2 운영 방식	주기·점검 허용	**화이트해커 책임하에 KISA에 취약점 신고**		**365일 24시간** 게시된 VDP 범위 내 **모든망/서비스 탐지 자율적 가능**
	조치·공개	기업 조치·공개 자율 **(강제력 없음)**	⇨	**의무** (예) 취약점 접수후 90일 이내 현행 망법에는 자율로 규정 되어 있어 개정 필요 **의무** (예) 패치조치 이후 취약점 내용/조치 방식과 기관·화이트 해커 의사 고려 실명 또는 익명 공개
	주체	**화이트해커 책임하에 취약점 신고**		**CVD·VDP : 기관, 기업**
3 참여 유인	공공	**해당 없음**		**실태평가 연계**
	민간			**보안인증 가점/공공입찰 우대** **사고시 과징금 연계**
	화이트 해커	소량의 보상금		**버그바운티 연계/보상** **지속 개선·확대**
4 법적 면책		사고시 면책 없음 (화이트해커 책임하에 취약점 발굴 및 신고)		**VDP 활동을 위한 상시 망 침입, 활동 과정에서 의도치 않은 개인정보 확인 등 면책**
5 기타(협력 및 인식개선)		- ※ 해킹 경진대회 등 일부 추진 중		화이트 해커, CVD·VDP 참여 기업 협력 네트워크 구축 홍보 캠페인, 정부표창 수여 등

1 대상 기관

○ 초기에는 우선 **참여기업·기관 모집**을 통해 시행하되 궁극적으로는 美와 유사하게 **공공**은 **단계적 제도화**(의무), **민간**은 **전면적인 참여 유도** 목표

2 운영 방식

○ 美·EU와 동일하게 대상 기관, 기업이 정한 **정책 범위 내** 화이트해커에게 **모든 망·서비스**에 대한 **취약점 자율 탐지 허용**

- 피신고 기업·기관은 신고 취약점에 대해 조치하고 조치 후 화이트해커와의 협의를 통해 일정시일 후 **기업·기관명/취약점** 등 **공개**
- 다만, **기업·기관·화이트해커 실명**은 본인의사 고려 **익명 공개를 허용**
- 아울러 **영세 기업·기관**에 대해서는 KISA 등을 통해 1차 취약점 신고 접수와 선별, 기관 전달 등을 수행, **취약점 조치 지원**도 병행*

* (예) AI취약점 자동 분석·검증 플랫폼 구축, API 보급 등 지원 병행

3 참여 유인

○ **공공**의 경우 수행근거 마련 이후 **실태평가**까지 연계, **민간은 보안인증** 가점·**공공조달 우대**·사고시 과징금 연계 등으로 초기 참여 유도

- 특히 **개보법**에 따른 **사고시 과징금**의 경우 새로 도입될 징벌적 과징금뿐 아니라 **동 제도 운영** 등 노력을 **과징금 감경 요소**로 반영*

* 美와 유사하게 과징금 산정시 고려하는 자율적인 개인정보 보호 노력(개인정보보호법 제64조의2 제4항제10호)에 CVD/VDP 운영 등 노력을 제도적 연계·반영

○ **화이트해커**에게는 취약점 **신고 포상금 제도 활성화**로 유인책 제공

4 보호 장치

○ 초기에는 **제3자 권리 침해**를 동반하지 않는 수준에서 **참여기업·기관-화이트해커** 상호 협의 기반하에 제한적 운영

○ 궁극적으로는 **관계 법률 개정**으로 **민·형사, 행정처벌 면제 장치** 완비

5 기타 협력 및 인식개선

○ 화이트해커, CVD·VDP 참여 기업, 기관, 정부간 **협력 네트워크** 구축 및 홍보 캠페인, 정부표창 수여 등 **인식 개선** 협력

Ⅳ. 추진 로드맵

◇ **美와 유사하게 시범 사업을 거쳐 공공·민간부문 보안을 총괄하는 주무 부처가 중심이 되어 순차적 법·제도 정비 추진**

< 참고 : 미국 CVD·VDP 제도화 과정 >

❶ 공공부문 시범사업 이후 → 공공부문 제도화 시작 (2016~2020)

- **(2016년) 美 국방부 시범사업 시행**(약 1,400명 해커참여, 138건 유효 취약점 발견으로 효용성 입증)
- **(2017년) 美 법무부, 공공기관 제도도입 참고 가이드라인** 제시 (**화이트 해커 고소금지 권고 내용** 포함)
- **(2020년) 美 사이버·인프라보안국** 모든 연방 행정기관에 VDP 수립 및 홈페이지 게시·운영을 의무화(CISA BOD 20-01 발령)

❷ 민간부문 도입 촉진 이후 → 민간·공공 제도화 완료 **(2020~2022)**

- **(2020년) 美 연방정부 공공조달 민간제품에 CVD·VDP 의무화**
- **(2022년) 美 법무부 화이트해커에 대해 기소금지 공식 선언**

1 시범 사업 추진(2026)

□ 민간은 과기정통부, 공공은 국정원 주도로 **시범 사업** 진행

○ **(예) 5~10개 선도기관**(기업 또는 공공기관)과 KISA, **화이트해커** 등 참여, CVD·VDP 제도의 **실효성·운영 가능성**을 **현실 환경**에서 검증

※ 신고, 조정, 패치, 공개 전 과정을 통합 시나리오로 시험

□ **시범사업 진행** 시 美·EU와 **유사한 환경** 조성, **국민 대대적 인식 환기**

○ **현행법 내**에서 추진하되 "**화이트 해커**의 취약점 탐색활동 중 의도치 않은 제3자 개인정보 확인", "개인정보처리자의 VDP 허용" 등에 대한 불명확한 법적 리스크를 관련 절차*를 거쳐 명확화, 대국민 인지

* **(예) 규제부처의 유권해석 또는 규제샌드박스 적극해석(합법 확인) 등**

⇨ **제도화 추진**에 앞서 그 **효과**와 함께 **사후조치 필요사항**을 사전에 확인

2 자율 기반 참여 확대 (~2027)

□ **(제도 설계) 시범 사업** 결과 기반, **상세 제도**(대상/절차/방식) **설계**

○ 민간(과기부), 공공(국정원) 제도 운영 상세 가이드라인 마련·배포 등

□ **(참여 유인) 공공 조달**(민간) 우대(조달청), **제도 운영**(공공) **예산** 지원(예산처), **실태평가**(공공) 연계(국정원), 사고 발생시 **과징금 경감**(개보위), 화이트 해커 버그 바운티 **운영기관 확대** 및 **포상금 상향**(과기부) 등

□ **(법제화 시작)** CVD/VDP 법적 근거 신설, 공공부문 의무화, **유인책 제공 등**을 위한 **관계부처 법령**(지침 포함) **개정안, 유관 제도 검토·마련**

검토 대상	개선사항 예시	관련부처
정보통신망법	▪ VDP에 근거한 선의의 화이트해커의 망접근 허용 및 처벌 금지 ※ 제48조제1항 및 동법 제71조 제1항 제11호 내지 제2항 제49조 및 동법 제71조 제1항 제14호 등 ▪ 정보통신망 안정성 확보 권고와 CVD 취약점 조치/공개 정합성 제고 보안패치 개발의 자율 조항 CVD의 취약점 조치 후 공개와 정합성 제고 ※ 제45조 제2항, 제47조의4 제4항 등 ▪ 이외 CVD·VDP 제도 근거 신설(기업의 신고·조치·공개 수립 및 게시(의무화, 권고), 제도 운영기관 및 조율·분장조정 기관 지정 근거마련 등)	과기정통부 + 법무부
개인정보 보호법	▪ CVD·VDP 운영 등 노력을 과징금 감경요소로 반영, 화이트해커·개인정보처리자 등 제도 참여자에 대한 개인정보보호법 위반 리스크 해소 지원	개인정보 보호위
국가 정보보안 기본지침	▪ 공공기관에 대한 VDP 제도에 대한 운영근거 마련, 단계적 제도화(의무) 등	국가정보원
저작권법 지침	▪ 제104조의2(기술적 보호조치의 무력화 금지) 예외사항에 VDP포함	문체부
민사/형사 리스크 관련	▪ 발생 가능한 민·형사 소송 리스크 해소를 위한 제도화 방안 검토 지원	법무부

⇨ **자율 참여기반 제한적 운영**을 통해 **민간·공공의 참여를 최대한 확대**하는 동시에 완전한 제도화를 위한 관계 법률 입법 시작

3 법제화(2단계 상황 고려 조속 추진)

□ **정보통신망법 등 관계 법률 개정 완료**

⇨ **美와 유사하게 공공 의무화, 민간**(조달 필수 요건화 등) **강력** 유인

Ⅴ. 향후 계획

□ **민간(과기부)·공공(국정원) CVD/VDP 시범 사업 추진** : '26.하반기

붙임 대한민국 AI행동계획(안) 관련 문구

⑨ 민간·공공 AI 보안 생태계 활성화 및 정보보호산업 자생력 확보

ㅇ 검토 배경

최근 국내 해킹 사고는 국가 배후 해킹그룹 등 체계적 공격에 의해 발생하고 있으며, 특히 보안인증을 획득한 기업조차도 해킹되고 있고 행정망까지 뚫리는 등 문제가 심각하다. 그러나 실제로 신고되는 해킹 사고는 일부에 불과한데, 이는 해킹 신고로 인한 과도한 비즈니스 리스크(최대 1천억원 과징금, 기업 이미지 손상 등)가 주요 원인이다. 그러나 보안은 기업·기관 활동의 필수 요소임에도 불구하고, 투자 우선순위에서 밀리는 경우가 많다. 보안 투자 효과는 장기적으로 나타나는 반면, 비용 부담은 즉각적이어서 적극적인 투자가 이루어지지 않기 때문이다. 현행 해킹 대응 체계의 단점(문서 위주의 사전인증제도, 신고 회피 및 소극적 보안 투자, 국산 외면)을 극복하려면, 기업·기관의 자발적 보안 활동을 촉진하는 정책과 재정적 인센티브를 함께 지원하는 것이 반드시 필요하다. 또한, AI안보 주권 확보를 위해서는 국내 정보보호 기업의 경쟁력 확보 또한 필수적이다. 국가와 민간이 함께 협력해 산업 맞춤형 AI 보안 역량을 높이고, 미래 지향적 AI 보안 기술기업을 집중 육성하는 노력이 병행되어야 한다.

ㅇ 정책 권고사항

- 국가AI전략위는 기존 사후 대응의 한계를 넘어 사전적이고 상시적인 정보통신망 보안 제도로의 패러다임 변화를 위해 美, EU가 이미 채택·운영 중인 취약점 신고·조치·공개 제도(CVD/VDP, Coordinated Vulnerability Disclosure,/ VDP(Vulnerability Disclosure Policy)에 대한 국내 민간·공공 도입 로드맵을 '26년 1분기까지 마련한다.

- 과기정통부와 국정원은 화이트해커[1]가 민간·공공분야 정보통신망 서비스 및 디지털 제품(소프트웨어, 하드웨어 등)의 보안 취약점을 사전에 발굴하는 활동을 합법적으로 수행할 수 있도록 해당 활동에 참여하는 피대상 기업·기관(공공기관 포함)을 지속 확대하는 한편, 참여 피대상 기업·기관을 대상으로 하는 시범사업을 '26년 4분기까지 우선 진행한다.

▪ 과기정통부와 국정원은 국가AI전략위가 마련한 로드맵에 따라 유관기관과 협력하여 민간·공공분야 정보통신망 서비스 및 디지털 제품의 보안 취약점을 효과적으로 발굴, 신고, 조치, 공개하는 협력적 가이드라인과 화이트해커의 참여 촉진 방안을 '26년 4분기까지 마련하고 CVD/VDP 관리 전문 기관을 지정한다.[2)]

▪ 과기정통부와 국정원은 '26년 4분기까지 수행된 시범사업 등의 결과를 바탕으로 민간·공공에 걸친 CVD/VDP 제도화를 위한 관련 법·제도 개선을 '27년 내 추진하며 법무부, 문체부, 개인정보위 등 관계부처는 이를 위한 소관 법률, 관계 하위법령 개정 등에 협조한다.

▪ 과기정통부, 국정원, 기획예산처, 조달청, 개인정보위는 디지털 제품 및 서비스에 대한 취약점 발굴·신고·공개 정책을 운영하는 민간 기업·공공기관에 대해 보안인증 가점, 실태평가 연계, 제도운영 예산 확보 지원, 정부 사업 입찰 우대, 사고 발생시 과징금 경감 등 다양한 인센티브를 제공하는 방안을 '26년 4분기까지 마련한다.

1) 화이트해커 : 침해사고 예방을 위한 선의의 목적으로 정보통신망 서비스 또는 디지털 제품의 취약점을 찾아 제보하는 개인 또는 조직(국가·공공기관, 대학교, 기업 등)

2) 보안 취약점 신고 포상제 개선 등 : 한국인터넷진흥원 등이 운영 중인 보안 취약점 신고 포상제(버그바운티)를 개선하여, 제조사 등 사업자가 보안 패치를 완료한 이후 공익 목적의 보안 연구자가 CVE(Common Vulnerabilities and Exposures) 발급 및 취약점 공개를 할 수 있도록 가이드라인을 정비한다. 제조사가 합리적인 기간(예: 90일) 내에 패치를 제공하지 않는 경우, 피해 최소화를 위한 제한적 공개(limited disclosure)를 연구자에게 제도적으로 허용하고, 이를 뒷받침하는 지원체계도 마련한다. 또한 유관기관(조정:한국인터넷진흥원 등, 법적 리스크: 검찰청·개인정보위 등)과 협의하여 선의의 취약점 발견자가 불이익을 받지 않게 하는 명확한 가이드라인을 만들고, 신고된 취약점에 대한 조치 상황을 투명하게 공개한다. CVD 관리 전문 기관으로는 한국인터넷진흥원 등을 지정, 기업과 보안 연구자 간 원활한 소통을 추진한다. 우리나라는 「정보통신망법」 등에서 주로 서비스 제공자·네트워크 운영자를 대상으로 침해사고 신고 의무를 규정하고 있어 사고 예방을 위한 취약점 신고 체계가 미비한 상황이므로, 관련 법령을 정비해야 할 필요가 있다.