KISA
INSIGHT
DIGITAL & SECURITY POLICY
2024 VOL. 01

미국 Cybersecurity 전략 및 실행계획 분석과 시사점

천곤웅, 김성훈

KISA 한국인터넷진흥원

KISA
INSIGHT
DIGITAL & SECURITY POLICY
2024 VOL. 01
2024년 1월

미국 Cybersecurity 전략 및 실행계획 분석과 시사점

천곤웅, 김성훈

CONTENTS

[작성]

한국인터넷진흥원(KISA) 미래정책연구실 정책개발팀

천곤웅 선임연구원 061-820-1124 konja11@kisa.or.kr
김성훈 팀장 061-820-1426 shkim@kisa.or.kr

[발간일] 2024년 1월 22일

[기획·발간처] 한국인터넷진흥원 미래정책연구실 정책개발팀

요약

▮ 미국 바이든 행정부는 '23년 3월 2일 트럼프 정부 이후 약 5년 만에 사이버 위협에 대응하기 위한 종합 전략인 새로운 국가 Cybersecurity 전략(NCS)을 발표

- 디지털 기술의 고도화로 한 세대 만에 전 세계의 혁신, 소통, 정보 공유 방식 등에 혁명을 불러일으켰지만 동시에 예측할 수 없는 위험을 초래할 가능성도 커지고 있음
- 사이버공간을 방어하기 위해 책임을 보다 효과적이고 공평하도록 재조정하고 보안, 복원력 및 유망 기술에 장기적 투자를 선호하도록 인센티브 제도를 재편성하기 위한 5가지 전략 발표

▮ Cybersecurity 전략의 비전 달성을 위한 실행계획(NCSIP)은 같은 해 7월 13일에 발표하여 전략에 대한 책임 기관, 협력 주체와 완료 시기를 공개

- NCSIP는 연방 정부의 사이버보안 전략 목표를 달성하기 위해 각 기관이 수행해야 할 역할과 국가사이버실(ONCD)의 역할을 명시함
- 연방정부는 민간 부문, 시민 사회, 각 주 및 지방정부, 국제 파트너 및 의회와 긴밀한 협력을 바탕으로 국가 사이버 보안 전략을 구현하기 위해 노력할 것임을 밝힘

▮ 미국 국가사이버실(ONCD)은 Cybersecurity 전략 발표 이후 가장 먼저 첫 번째 전략 과제인 「U.S. Cyber Trust Mark Program」을 발표

- 국가 사이버 노동력 및 교육 전략(NCWES)을 발표하며 사이버 인력 양성과 교육을 위해 연방정부의 주요 기관들과 파트너십을 체결
- 오픈소스 소프트웨어 보안 이니셔티브(OS3I)를 설립하고 CISA, NSF, NIST 등과 협력하여 오픈소스 소프트웨어 보안 우선순위를 설정하고 정책 솔루션을 개발 중
- 국내 사이버보안 정책도 보안 규제개선, 사이버 10만 인재 양성 방안, 안전한 오픈소스 활용 등 미국의 NCS와 유사한 사이버보안 관련 정책들을 수립하여 수행 중

▮ 디지털 전환 가속화로 사이버 위협이 산업 · 사회 · 안보 全 영역으로 확대 및 지능화되고 있기 때문에 민간 · 공공 협력을 바탕으로 하는 포괄적 대응 필요

- 선제적 대응이 가능한 사이버 방어 정책 전환이 요구되며 이를 위해 사이버 공격으로 피해가 발생되기 이전에 공격자의 의도를 미리 분석하여 사전 조치가 이루어져야 함
- 민관협력 체계 구축을 바탕으로 사이버 위기 대응을 위한 新기술 R&D 투자와 민간기업의 Cybersecurity 역량 강화를 도모하여 사이버 위협 공동 대응 체계 구축이 필요

I

국가 Cybersecurity 전략 및 실행계획

▮ 미국 「국가 Cybersecurity 전략」의 5가지 전략 및 구현 방안

• 바이든 행정부는 트럼프 정부 이후 약 5년 만에 새로운 「국가 Cybersecurity 전략(NCS, National Cybersecurity Strategy)」을 발표('23.3.2.)

– 국가안보전략(National Security Strategy) 보고서 및 국가방위전략(National Defense Strategy) 보고서를 기반으로 민간 부문과의 협력을 통해 개발

• 해당 전략(NCS)은 바이든 정부 출범 이후 사이버 위협에 대응하기 위해 시행해 온 다양한 사이버보안 관련 정책들을 통합하고 계승하고 있는 종합 전략

[표 1] NCS 개발에 반영된 미국 주요 정책

구 분	주요 내용
Excutive Order (EO, 행정명령)	• "국가 사이버안보 개선"에 관한 행정명령 14028호(EO-14028) • "연방 네트워크 및 주요 인프라의 사이버안보 강화"에 관한 행정명령 13800호 • "주요 인프라의 사이버보안 개선"에 관한 행정명령 13636호
NSM[1] (국가안보각서)	• "주요 인프라 통제 시스템을 위한 사이버보안 개선"에 관한 국가안보각서 5호 • "국가 안보, 국방부 및 정보 공동체 시스템을 위한 사이버보안 개선"에 관한 국가안보각서 8호
Memorandum (정책지침)	• "핵심 인프라의 안보 및 회복탄력성"에 관한 대통령정책지침 21호 • "미국의 사이버 사고 관련 조정"에 관한 대통령정책지침 41호 • "우주 시스템을 위한 사이버보안 원칙"에 관한 우주정책지침 5호
Initiative (이니셔티브)	• 국가 인공지능 이니셔티브 • 국가 사이버안보 이니셔티브 2008
National Strategy (국가전략)	• 5G 보안을 위한 국가 전략

[1] National Security Memorandum

- 미국은 사이버안보는 경제, 국방, 주요 인프라 운영, 민주주의 제도 강화 등 모든 분야에 필수적이며 디지털 범죄, 디지털 생태계를 위협하는 세력을 좌절시키고 회복력을 확보하는 것이 중점이라는 인식을 바탕으로 다음과 같이 사이버안보 분야의 전략적 환경과 사이버공간 복원력 강화를 위한 접근방법을 설명

– (전략적 환경) SW 및 시스템의 복잡성 증대와 인공지능의 보급으로 위험성이 더욱 커지고 있으며 디지털 기술은 예측하지 못한 새로운 위험을 초래할 가능성이 존재하기에 사이버 공간의 복원력 확보 필요

– (접근방법) 사이버공간을 방어하는 사이버보안에 대한 책임을 보다 효과적이고 공평하도록 재조정하고 보안, 복원력 및 유망 기술에 장기적 투자를 선호하도록 인센티브 제도를 재편성

- 디지털 생태계를 구성하는 이해관계자 간의 긴밀하고 지속적인 협력을 위해 5가지 전략을 발표하였으며 해당 전략들을 사이버 공간의 안전과 복원력을 강화하는 목표로 삼음

– (5가지 전략) △ 주요 인프라 방어 △ 위협 행위자 저지 및 무력화 △ 보안 및 복원력 강화를 위한 시장의 힘 형성 △ 복원력 있는 미래에 투자 △ 공동 목표 추구를 위한 국제 파트너십 구축

- NCS 전략의 비전 달성을 위한 국가 Cybersecurity 전략 실행계획(NCSIP, National Cybersecurity Strategy Implementation Plan)을 발표하고 세부 계획에 대한 책임 기관, 협력 주체와 완료 시기(회계연도 기준)를 작성하여 공개('23.7.13.)

– NCSIP는 연방정부의 Cybersecurity 전략 목표를 달성하기 위해 각 기관이 수행해야 할 역할과 국가사이버실(ONCD)의 역할을 명시

– 연방정부는 민간 부문, 시민 사회, 각 주 및 지방정부, 국제 파트너 및 의회와 긴밀한 협력을 바탕으로 국가 Cybersecurity 전략을 구현하기 위해 노력할 것을 밝힘

1-1 주요 인프라 방어(Defend Critical Infrastructure)

- 사이버 공간의 위험과 책임을 공평하게 분배하고 디지털 생태계에 필요한 기본적인 수준의 보안과 복원력을 제공할 수 있는 지속적이고 효과적인 공동 방어 모델을 운영하는 것에 목표를 두고 있음

- Cybersecurity 정책을 대규모로 추진할 수 있는 규정과 일관되고 예측 가능한 Cybersecurity 규제 프레임워크를 마련하기 위해 민간 분야와 협력을 통한 혁신을 장려

- 주요 인프라의 소유자와 운영자, 연방 기관, 제품 · 서비스 공급업체, 기타 이해관계자가 대규모로 효과적으로 협력할 수 있도록 새롭고 혁신적인 역량을 구축하여 연방 기관 간 협력 능력 강화를 추구

▮ 전략 1.1 : 국가 안보 및 공공 안전을 지원하기 위한 사이버안보 요건 신설 (Establish Cybersecurity Requirements to Support National Security and Public Safety)

- (주요 인프라의 사이버안보 규제 마련) 주요 부문에 필요한 사이버안보 요건을 설정하기 위해 기존의 정부 권한들을 사용할 방침이며 해당 권한을 조율하여 사용할 것을 권장할 예정

- 사이버안보와 관련된 규정 및 표준은 성능에 초점을 맞추고 CISA의 사이버안보 성과 목표와 NIST의 주요 인프라 사이버안보를 위한 프레임워크 등을 기존의 사이버안보 프레임워크와 조율할 예정
- 정부는 클라우드 컴퓨팅 산업 및 기타 제3의 서비스 부문의 사이버안보 관행을 강화하기 위해 관할 당국의 격차를 파악하고 이를 해소하기 위해 업계, 의회, 규제 기관들과 협력을 강화

• (기존 · 신설 규정 간의 조화 및 간소화) 국가사이버실(ONCD), 예산관리실(OMB)와 협력하여 사이버안보 규제 요건의 피해를 방지하기 위해 국가 간 규제 조화를 추진할 방침

• (규제 기관의 보안 비용 지원) 주요 인프라 부문은 수익에 따라 사이버 보안 비용을 감당할 여력이 다르기 때문에 공정한 기회의 장을 조성하여 사이버 보안에 대한 필수 투자를 장려하고 규제 프레임워크 개발 예정

[표 2] NCS 전략 1.1 실행계획 주요 내용

NCS 1.1 실행계획(NCSIP)	책임기관	완료기한
1.1.1 사이버 규제 조화를 위한 계획 수립 (Establish an initiative on cybersecurity regulatory harmonization)	ONCD (국가사이버실)	1분기 FY24
1.1.2 주요 기반시설 부분에 걸친 사이버 보안 요구사항 설정 (Set cybersecurity requirements across critical infrastructure sectors)	NSC (국가안보회의)	2분기 FY25
1.1.3 규제 조정을 알리기 위해 기관의 프레임워크 및 국제 표준 활용 확대 (Increase agency use of frameworks and international standards to inform regulatory alignment)	NIST (표준기술연구소)	1분기 FY25

• 이니셔티브 1.1.1 : 사이버 규제 조화를 위한 계획 수립

- 국가사이버실(ONCD)는 예산관리실(OMB)와 협력하여 독립 및 행정부 규제 기관을 위한 사이버 보안 포럼 및 협력을 통해 중요 인프라에 대한 기본 사이버보안 요구 사항을 조화시기 위한 노력을 이행
- 국가사이버실은 정보 요청(RFI)를 통해 비정부 이해 관계자를 참여시켜 규제 중복으로 인한 기존 문제를 이해하고 기본 요구 사항에 대한 상호주의 프레임워크를 탐색

• 이니셔티브 1.1.2 : 주요 기반시설 부분에 걸친 사이버 보안 요구사항 설정

- 국가안보국(NSA)이 주도하는 정책 결정 프로세스를 통해 SRMA[2]와 규제 기관은 해당 산업의 사이버 위험을 분석하고 기존 권한을 사용하여 해당 부문의 위험을 완화와 부문별 요구 사항을 설명, 권한의 격차를 식별하여 이를 해결하기 위한 제안사항을 개발하는 방법에 대해 설명

• 이니셔티브 1.1.3 : 규제 조정을 알리기 위해 기관의 프레임워크 및 국제 표준 활용 확대

- NIST는 해당 프레임워크에 대한 중요 업데이트인 CSF[3] 2.0을 개발하며 최종 CSF 2.0을 발표하고 연방기관의 요청에 따라 규정을 국제 표준 및 NIST CSF와 일치시키기 위한 기술 지원을 제공

2 Sector Risk Management Agency : 부문별 위험 관리 기관
3 Cybersecurity Framework

▮ 전략 1.2 : 민 · 관 협력 확대(Scale Public-Private Collaboration)

• CISA는 SRMA와 협력하여 시스템과 자산을 보호할 책임이 있는 각 분야의 인프라 소유주와 운영자에게 지원을 제공하고 ISAO*, ISAC**는 사이버 방어 작전을 수행할 것

* 정보 공유 및 분석 조직, ** 부문별 정보 공유 및 분석 센터

• 연방정부는 SRMA와의 협력과 투자를 강화하여 주요 인프라 소유자 및 운영자의 요구에 선제적으로 대응할 수 있도록 지원하고 SMRA 간의 격차를 파악하여 보완할 계획

- SRMA의 역량 구축에 투자하여 인프라 보안 및 복원력을 강화하고 제3자 협업 메커니즘 지원과 사이버 환경을 재구성할 수 있는 능력을 갖춘 SW/HW 및 서비스 제공업체와의 전략적 협력을 심화

[표 3] NCS 전략 1.2 실행계획 주요 내용

NCS 1.2 실행계획(NCSIP)	책임기관	완료기한
1.2.1 보안 기반의 설계 및 보안 기술 기본 설계 채택 촉진을 위한 공공-민간 파트너십 확대(Scale public-private partnerships to drive development and adoption of secure-by-design and secure-by-default technology)	CISA (사이버보안·인프라보안국)	4분기 FY24
1.2.2 주요 기반시설 섹터 및 SRMA 지정에 대한 권장 사항 제공 (Provide recommendations for the designation of critical infrastructure sectors and SRMAs)	CISA (사이버보안·인프라보안국)	1분기 FY24
1.2.3 CISA가 기존 보고 체계 또는 개별 포털의 잠재적 창의성을 활용하여 SRMA의 섹터별 시스템 및 프로세스를 통합 및 운영할 수 있는 방법 평가 (Evaluate how CISA can leverage existing reporting mechanisms or the potential creation of a single portal to integrate and operationalize SRMAs's sector-specific systems and processes)	CISA (사이버보안·인프라보안국)	3분기 FY24
1.2.4 새롭게 개선된 정보 공유 및 협력 플랫폼, 절차 및 체계를 위한 기회 조사 (Investigate opportunities for new and improved information sharing and collaboration platforms, processes, and mechanisms)	CISA (사이버보안·인프라보안국)	1분기 FY26
1.2.5 SRMA 지원 역량 구축 (Establish an SRMA support capability)	CISA (사이버보안·인프라보안국)	2분기 FY25

• 이니셔티브 1.2.1 : 보안 기반의 설계 및 보안 기술 기본 설계 채택 촉진을 위한 공공-민간 파트너십 확대

- CISA는 기술 제조업체, 교육자, 비영리 조직 등 기타 기관과의 공공-민간 파트너십을 주도하여 설계 및 안전한 소프트웨어 및 하드웨어의 개발 및 채택을 장려할 것

- CISA는 NIST, SRMA를 포함한 연방 기관, 민간 부문과 협력하여 정부 표준 및 관행을 활용하기 위한 기본 보안 원칙을 개발할 것

• **이니셔티브 1.2.2 : 주요 기반시설 섹터 및 SRMA 지정에 대한 권장 사항 제공**

- 연방 고위 리더십 위원회를 통해 합의된 SRMA의 기능을 검토하고, 적절한 경우 민간 부문 파트너와 협의하여 중요 인프라 부문의 SRMA에 대한 권장 사항을 국토안보부 장관에게 보고

• **이니셔티브 1.2.3 : CISA가 기존 보고 체계 또는 개별 포털의 잠재적 창의성을 활용하여 SRMA의 섹터별 시스템 및 프로세스를 통합 및 운영할 수 있는 방법 평가**

- CISA는 SRMA와 협력하여 정보공유 체계에 존재하는 격차를 파악하여 SRMA 및 기타 연방 파트너 간의 정보 교환을 위한 상호 운용 시스템에 대한 요구 사항을 제시할 것
- 정보공유 기능이 없는 경우 CISA와 SRMA는 협력하여 정보공유 프로세스를 개발 할 예정

• **이니셔티브 1.2.4 : 새롭게 개선된 정보 공유 및 협력 플랫폼, 절차 및 체계를 위한 기회 조사**

- CISA는 SRMA와 부문 조정 위원회, 정보공유 및 분석센터(ISAC), 정보공유 및 분석조직(ISAO), 신흥 부문 협력 이니셔티브 및 공공-민간 협력을 위한 성숙 모델 개발을 위해 협력할 것

• **이니셔티브 1.2.5 : SRMA 지원 기능 구축**

- CISA는 SRMA를 지원하기 위한 사무소 기능을 수립하여 사무소 지원에 대한 요구 사항과 우선순위를 정의하고 공유 서비스에 대한 옵션 등을 해당 정보를 CISA 서비스 카탈로그에 업데이트 예정

▮ 전략 1.3 : 연방 사이버안보센터 통합(Intergrate Federal Cybersecurity Centers)

• 연방 사이버안보센터(IFCC, Integrate Fedral Cybersecurity Centers)는 국토방위, 법 집행, 정보, 외교 경제 및 군사 등 전반에 걸쳐 정부 전체 기능을 융합하는 협업 노드의 역할을 수행할 예정

- 연방 정부, 민간 부문 및 국제 파트너와 함께 사이버 방어 계획 및 운영을 통합하기 위해 CISA에 합동 사이버방어 협력체(JCDC, Joint Cyber Defense Collaborative)[4]를 설립하여 목표를 향한 진전을 이룬바 있음
- 법 집행 및 기타 조정을 위해 국가 사이버 수사 합동 태스크 포스(NCIJTF, National Cyber Investigative Joint Task Force)의 역량을 강화하고 인텔리전스 수집, 분석 및 파트너십을 조정하는 사이버 위협 정보 통합 센터(CTIIC, Cyber Threat Intelligence Integration Center)의 역할을 활성화 할 것

[표 4] NCS 전략 1.3 실행계획 주요 내용

NCS 1.3 실행계획(NCSIP)	책임기관	완료기한
1.3.1 연방 사이버 보안 센터 및 관련 사이버 센터의 협력을 위해 필요한 역량과 계획을 신속하고 규모에 맞게 평가 및 개선 (Assess and improve Federal Cybersecurity Centers and related cyber centers capabilities and plans necessary for collaboration at speed and scale)	ONCD (국가사이버실)	4분기 FY23

4 2021년 국방수권법에 의해 설립된 사이버 공간의 방어와 글로벌 사이버 커뮤니티를 통합하는 공공-민간의 사이버안보 협력체이며 미국의 사이버안보 주요 부처, 국가안보국, FBI 등이 전부 포함되며 CERT로 알려진 국제 사고 대응 팀과 협력 수행, 핵심 기능은 ① 사이버방어 작전 계획 개발 및 조정, ② 공공과 민간의 협업 및 융합, ③ 모든 이해 관계자에게 사이버 방어지침 전달

• **이니셔티브 1.3.1 : 연방 사이버보안 센터 및 관련 사이버센터의 협력을 위해 필요한 역량과 계획을 신속하고 규모에 맞게 평가 및 개선**

– 국가사이버실은 연방 사이버 보안 센터 및 관련 사이버 센터를 검토하여 역량의 격차와 기타 주요 결과를 식별 할 것

▮ 전략 1.4 : 연방정부의 사이버 사건 대응 계획 및 프로세스 개선 (Update Federal Incident Response Plans and Processes)

• 연방 정부는 통일되고 조율된 범정부 차원의 대응책을 제시하여 사이버 위협 발생 시 어떤 정부 기관에 어떤 목적으로 연락해야 하는지 파악하고 있어야 하며 지원 형태에 대한 명확한 지침도 제공해야 함

– 사건 발생 시 중요 인프라에 대한 사이버 사고 보고법(CIRCIA, Cyber Incident Reporting for Critical Infrastructure Act)에 따라 피해 대상 주체가 사이버 사고에 대해 CISA에 보고해야 함

– 미 국토부 산하 조직인 사이버 안전 심의 위원회(CSRB, Cyber Safety Review Board)를 명문화된 법안으로 통과 시켜 중대 사건에 대한 포괄적인 검토를 수행하는데 필요한 권한을 부여할 예정

– 중대 사이버 사고 발생 후 연방 정부는 사이버 안전 심의 위원회를 통해 해당 사고를 통해 개선점을 파악하도록 할 계획

[표 5] NCS 전략 1.4 주요 내용

NCS 1.4 실행계획(NCSIP)	책임기관	완료기한
1.4.1 국가 사이버 사고 대응 계획 업데이트 (Update the National Cyber Incident Response Plan(NCIRP))	CISA (사이버보안,인프라보안국)	1분기 FY25
1.4.2 사이버사고신고법 원칙 최종본 공표 (Issue final Cyber Incident Reporting for Critical Infrastructure Act(CIRCIA))	CISA (사이버보안,인프라보안국)	4분기 FY25
1.4.3 사이버 사고 대응을 개선하기 위한 훈련 시나리오 개발 (Develop exercise scenarios to improve cyber incident response)	ONCD (국가사이버실)	1분기 FY24
1.4.4 사이버 안전 검토 위원회를 필수 조직으로 성문화하기 위한 법안 초안 작성 (Draft legislation to codify the Cyber Safety Review Board(CSRB) with the required authorities)	DHS (국토안보부)	2분기 FY23

• **이니셔티브 1.4.1 : 국가사이버사고 대응 계획(NCIRP) 업데이트**

– CISA는 ONCD와 협력하여 “대통령 정책지침 41호”[5]에 명시된 국가 사이버 사고 대응계획(NCIRP)을 업데이트하는 프로세스 및 시스템을 강화하고 연방기관의 역할과 기능에 대한 명확한 지침까지 수립할 것

• **이니셔티브 1.4.2 : 사이버 사고 신고법(CIRCIA) 원칙 최종본 공표**

– CISA는 사이버 사고 신고법(CIRCIA) 구현을 위해 SRMA, 법무부 및 기타 연방기관과 협의하여 사이버 사고 신고법에 대한 최종본 게시와 사건 보고서 공유 및 효과적인 사후조치 발전을 위한 프로세스 개발할 예정

5 미국의 사이버 사고 관련 조정에 관한 대통령 정책지침

• **이니셔티브 1.4.3 : 사이버 사고 대응을 개선하기 위한 연습 시나리오 개발**

– ONCD는 기관 및 기타 이해당사자들과 협력을 바탕으로 기관 간 사이버 사고에 대한 범정부적 대응을 지속적으로 개선할 수 있도록 모의 훈련 시나리오를 개발할 것

• **이니셔티브 1.4.4 : 사이버 안전 검토 위원회를 필수 조직으로 성문화하기 위한 법안 초안 작성**

– 연방정부는 의회와 협력하여 국토안보부 내에서 CSRB를 성문화하고 주요 사건에 대한 포괄적인 검토를 수행함에 필요한 권한을 부여하는 법안을 통과시킬 것

▮ 전략 1.5 : 연방 정부 방어의 현대화(Modernize Federal Defenses)

• (연방의 사이버 방어) 연방민간행정기관(FCEB, Federal Civil Executive Branch)[6]은 자체 IT 및 OT 시스템을 관리하고 보호할 책임이 있으며 방어에 대한 집합적 접근 방식을 통해 기관의 개별 권한 및 역량에 맞는 연방 사이버안보 모델을 구축해야 함

– 예산관리실은 CISA와 협력하여 집단 운영 방어, 중앙 집중식 공유 서비스의 가용성, 소프트웨어 공급망 위험 완화 등 연방의 시스템을 보호하기 위한 계획을 개발할 것

– NIST는 소프트웨어 공급망 위험 완화를 위한 SBOM(Software Bills of Material), 보안 소프트웨어 개발 프레임워크, 오픈 소스 소프트웨어 보안 등을 개선할 것

• (연방 시스템의 현대화) 연방 정부는 취약한 IT 및 OT 시스템을 교체하거나 업데이트해야 하며 제로 트러스트 아키텍처 전략을 통해 각 개별 연방민간행정기관(FCEB)이 다단계 인증을 구현하고, 데이터 암호화, 전체 공격 영역에 대한 가시성 확보, 인증 및 액세스 관리, 클라우드 보안 도구를 채택하도록 지시

– 예산관리실(OMB)은 유지 관리 비용이 많이 들고 방어하기 어려운 시스템을 제거하기 위한 연방 정부의 노력에 우선순위를 두어 연방민간행정기관의 기술 현대화를 가속화하기 위한 계획의 개발을 주도할 것

– 연방 시스템을 현대화하고 안전한 기술로 교체하면 연방 정부의 전체의 사이버안보 태세를 강화할 수 있고 디지털 서비스의 보안 및 회복력을 개선 할 것으로 기대

• (국가 안보 시스템 방어) 국가 안보 시스템(NSS, National Security System)은 연방 정부의 민감한 데이터 일부를 저장, 사이버 범죄자 및 국가의 적들의 광범위한 사이버 및 물리적 위협으로부터 보호되어야 함

– 국가안보시스템의 책임자인 국가안보국(NSA, National Security Agency) 국장은 예산관리실과(OMB)과 협력하여 대통령 국가 안보 각서 대통령 국가안보각서 NSM-8에 나와있는 강화된 사이버안보 요구사항인 연방민간행정기관(FCEB)의 국가 보안 시스템(NSS) 계획을 개발할 것

6 연방민간행정기관(FCEB) : CISA의 권한에 영향을 받는 연방 내에 다양한 공공, 민간 행정기관들을 통틀어서 말하며 각종 이사회, 위원회, 공사, 재단, 부처, 협의회, 봉사단 등으로 구성

[표 6] NCS 전략 1.5 실행계획 주요 내용

NCS 1.5 실행계획(NCSIP)	책임기관	완료기한
1.5.1 미분류 연방민간행정기관 시스템 보안 (Secure unclassified Federal Civilian Executive Branch(FCEB) system)	OMB (예산관리실)	2분기 FY24
1.5.2 연방민간행정기관 기술 현대화 (Modernize Federal Civilian Executive Branch(FCEB) technology)	OMB (예산관리실)	4분기 FY24
1.5.3 연방민간행정기관에 대한 국가보안시스템(NSS) 확보 (Secure National Security System(NSS) at Federal Civilan Executive Branch(FCEB) agencies)	NSA (국가안보국)	4분기 FY24

• **이니셔티브 1.5.1 : 미분류 연방민간행정기관(FCEB) 시스템 보안**

- OMB는 CISA와 협력하여 집단 운영 방어를 통해 분류되지 않은 연방민간행정기관 시스템을 보호하고 중앙 집중식 공유 서비스, 기업 라이선스 계약 및 소프트웨어 공급망 위험 완화의 사용 확대를 촉진할 것

• **이니셔티브 1.5.2 : 연방민간행정기관(FCEB) 기술 현대화**

- OMB는 유지비용이 많이 들고 방어하기 어려운 레거시 시스템을 제거하기 위한 연방정부의 노력에 우선순위를 두고 연방민간행정기관 기술 현대화를 가속화하기 위한 계획 개발을 주도할 것

• **이니셔티브 1.5.3 : 연방민간행정기관(FCEB)에 대한 국가보안시스템(NSS) 확보**

- NSA는 국가보안시스템(NSS)에 대한 국가 관리자의 책임을 수행하는 동시에 연방민간행정기관에서 국가보안시스템의 문제를 해결하기 위한 계획을 개발하고 실행할 것

1-2 위협 행위자 저지 및 해체(Disrupt and Dismantle Threat Actors)

• 미국은 자국의 이익을 위협하는 행위자를 저지하고 해체하기 위해 모든 국력을 동원할 것이며 정부의 목표는 악의적 행위자가 지속적인 사이버 기반 공격을 단행하지 못하게 만드는 데 있음

• 위협 행위자를 저지하기 위해 정보 공유 개선, 대규모 캠페인, 적국의 미국 기반 인프라 사용 금지, 글로벌 랜섬웨어 저지 캠페인 등을 통해 공공 및 민간 부문의 협력을 강화할 것

▮ 전략 2.1 : 연방정부 차원의 통합적인 저지활동(Integrate Federal Disruption Activities)

• 통합 저지활동은 사이버 범죄 활동의 수익성을 제거하여 악의적인 사이버 활동에 관여하는 외국 정부가 사이버 범죄가 더 이상 목표 달성에 효과적인 수단이 아님을 인식하도록 함을 목표로 하고 있음

- 연방정부는 통합 저지 활동의 규모와 속도를 높이기 위해 지속적이고 조정된 운영을 가능하게 하는 기술 및 조직 플랫폼을 추가적으로 개발 예정

- 국가 사이버 수사 합동 태스크 포스(NCIJTF, Naitonal Cyber Investigative Joint Task Force)가 범정부적 통합 저지 캠페인을 실행하기 위한 중심 기관 역할을 할 예정

[표 7] NCS 전략 2.1 실행계획 주요 내용

NCS 2.1 실행계획(NCSIP)	책임기관	완료기한
2.1.1 업데이트된 국방부 사이버 전략 발행 (Publish an updated DOD Cyber Strategy)	DOD (국방부)	1분기 FY24
2.1.2 국가사이버수사공동대책반 역량 강화 (Strengthen the National Cyber Investigative joint Task Force(NCIJTF) capacity)	FBI (연방수사국)	4분기 FY25
2.1.3 저지 활동 전용 조직 플랫폼 확대 (Expand organizational platforms dedicated to disruption campaigns)	DOJ (법무부)	1분기 FY25
2.1.4 사이버 범죄 및 사이버 지원 범죄 저지 및 방지를 위한 법률 제안 (Propose legislation to disrupt and deter cyber crime and cyber-enabled crime)	DOJ (법무부)	4분기 FY23
2.1.5 저지 활동의 속도 및 규모 증대 (Increase speed and scale of disruption operations)	FBI (연방수사국)	2분기 FY24

• **이니셔티브 2.1.1 : 업데이트된 국방부 사이버 전략 발행**

– 미 국방부는 국가안보전략, 국방 전략 및 사이버 보안 전략과 연계하여 업데이트된 국방부 사이버 전략을 미국에 위협을 가하는 능력을 가진 국가 및 행위자가 제기하는 문제에 초점을 맞춰 개발할 것

• **이니셔티브 2.1.2 : 국가 사이버 수사 공동 대책반 역량 강화**

– 국가 사이버 수사 공동 대책반의 더 빠른 속도와 더 큰 규모로 악의적 행위자들의 교란 및 저지하는 캠페인 역량을 강화 할 것

• **이니셔티브 2.1.3 : 저지 활동 전용 조직 플랫폼 확대**

– 미 법무부는 사이버 위협을 전담하는 조직 플랫폼을 확장하여 사이버 업무 자격을 갖춘 변호사 수를 증가시켜 사이버 범죄자, 국가적 적대자 및 관력 조력자에 대한 중담 캠페인의 규모와 속도를 증대할 것

• **이니셔티브 2.1.4 : 사이버 범죄 및 사이버 지원 범죄 저지 및 방지를 위한 법률 제안**

– 법무부는 부처 간 파트너와 협력하여 제정될 경우 사이버 범죄를 방해하고 억제하는 미국 정부의 역량을 강화할 일련의 목표를 다룬 입법안을 개발할 것

• **이니셔티브 2.1.5 : 저지 활동의 속도 및 규모 증대**

– 국가 사이버 수사 합동 태스크포스(NCIJTF), 법 집행 기관, 사이버 사령부 및 기타 정보 커뮤니티들은 협력을 통해 저지 활동의 속도와 규모를 증대하기 위한 작업을 조정하고 실현하기 위한 옵션 개발을 주도할 것

▮ 전략 2.2 : 위협 행위자 저지를 위한 민 · 관 협력 강화 (Enhance Pubilc-Private Operational Collaboration to Disrupt Adversaries)

• 적대적 활동에 대해 민간 부문이 수집한 정보는 부분적으로 연방정부보다 더 포괄적이고 상세하며 위협을 추적하는 역량이 빠르게 발전하고 있기에 악의적 활동을 차단하기 위해서는 민 · 관 협력이 중요

- 국가 사이버 포렌식 교육연합(NCFTA, National Cyber-Forensics and Training Alliance)과 같은 연방정부와의 운영 협력 허브 역할을 할 수 있는 비영리 파트너 조직을 통해 공동 대응하는 것을 권장
- 위협 관련 협업은 관련 메인 허브에서 컨트롤하며 소수의 신뢰할 수 있는 운영자로 구성된 민첩한 셀 형태를 취해야 하고 셀 구성원은 가상 협업 플랫폼을 사용하여 적을 방해하기 위해 신속하게 대응할 방침

[표 8] NCS 전략 2.2 실행계획 주요 내용

NCS 2.2 실행계획(NCSIP)	책임기관	완료기한
2.2.1 공공-민간 협업을 통한 적대적 행위 증가에 대한 체계 식별 (Identify mechanisms for increased adversarial disruption through public-private operational collaboration)	ONCD (국가사이버실)	2분기 FY24

• 이니셔티브 2.2.1 : 공공-민간 협업을 통한 적대적 행위 증가에 대한 체계 식별

- ONCD는 기관 및 민간 부문 파트너와 협력하고 기존 메커니즘을 활용하여 악의적인 사이버 행위자의 혼란을 증가시키는 것을 목표로 운영 협력을 개선할 수 있는 기회를 식별할 것

▮ 전략 2.3 : 정보 공유 및 피해 알림 속도와 규모의 향상 (Increase the Speed and Scale of Intelligence Sharing and Victim Notification)

• 사이버 위협 공동 대응에 대한 인식은 높아졌지만 정부만이 수집할 수 있는 고유한 국가 정보가 있고 해당 위협 정보를 신속히 알리기 위한 사이버 위협 정보를 공유하는 속도와 범위를 개선할 것

- 섹터별 위험 관리 기관(SRMA)는 CISA, 법 집행 기관, 사이버위협정보통합센터(CTIIC)와 협력하여 부문별 정보의 필요와 우선순위를 파악하고 관련 데이터를 파트너 모두에게 공유하는 절차를 개발할 예정

[표 9] NCS 전략 2.3 실행계획 주요 내용

NCS 2.3 실행계획(NCSIP)	책임기관	완료기한
2.3.1 부문별 인텔리전스 요구사항 및 우선순위 식별 및 운영 (Identfy and operationalize sector-specific intelligence needs and priorities)	NSC (국가안보회의)	1분기 FY25
2.3.2 주요 기반시설 소유 및 운영자에게 사이버 위협 인텔리전스 및 데이터 제공 장벽 제거 (Remove barriers to delivering cyber threat intelligence and date to critical infrastructure owners and operators)	ODNI (국가정보국)	3분기 FY24

• 이니셔티브 2.3.1 : 부문별 인텔리전스 요구사항 및 우선순위 식별 및 운영

- 국방수권법 섹션 9002(c)(1)에 명시된 요구사항에 따라 NSC는 SRMA가 부문별 인텔리전스 요구사항과 우선순위를 식별하기 위해 합의된 접근방식을 수립하기 위한 정책 결정 프로세스를 주도할 것

• **이니셔티브 2.3.2 : 주요 기반시설 소유 및 운영자에게 사이버 위협 인텔리전스 및 데이터 제공 장벽 제거**

– 행정명령 13636[7] 시행 이후, 국가정보국장은 법무부 및 국토부와 협력하여 중요 인프라 소유자 및 운영자와 사이버 위협 인텔리전스를 공유하기 위한 정책 및 절차를 검토하고 인텔리전스 접근 확대의 필요성을 평가할 것

▮ 전략 2.4 : Prevent Abuse of U.S.-Based Infrastructure (미국 기반 인프라 악용 방지)

• 악의적 행위자들이 스파이 활동을 하는데 있어 미국에 기반을 둔 디지털 서비스를 악용하고 있어 연방정부는 피해자가 시스템의 악용을 간편히 신고하게 하고 악용을 위한 접근을 어렵게 만들 것

– 사이버안보에 대한 위험 기반 접근 방식을 IaaS 제공업체 전반에 채택하고 시행하는 것을 우선순위로 삼을 계획

[표 10] NCS 전략 2.4 실행계획 주요 내용

NCS 2.4 실행계획(NCSIP)	책임기관	완료기한
2.4.1 IaaS 공급자 및 리셀러를 위한 요구사항, 표준 및 절차에 대한 제안 규칙 제정 공지사항 공표 (Publish a Notice of proposed Rulemaking on requirements, standards, and procedures for Infrastructure-as-a-service (IaaS) providers and resellers)	DOC (상무부)	4분기 FY23

• **이니셔티브 2.4.1 : IaaS 공급자 및 리셀러를 위한 요구사항, 표준 및 절차에 대한 제안 규칙 제정 공지사항 공표**

– 상무부는 IaaS 공급자 및 리셀러에 대한 요구사항과 면제 가능한 위험 기반 예방 접근방식을 결정하기 위한 표준 및 절차를 설명하는 행정명령 13984를 구현하는 제안된 규칙 제정 통지를 게시할 것

▮ 전략 2.5 : 사이버 범죄 대응 및 랜섬웨어 퇴치(Counter Cybercrime, Defeat Ransomware)

• 랜섬웨어는 연방정부의 국가안보 및 주요 인프라와 필수 서비스에 심각한 장애를 일으켰으며 러시아, 이란, 북한과 같은 적성국들이 랜섬웨어를 통해 암호화폐로 대금을 갈취하고 수익금을 세탁하고 있음

• 연방정부는 랜섬웨어 퇴치를 위해 다음 네 가지 활동과 함께 국력의 모든 요소를 사용할 것

– (1) 다른 국가와의 협력으로 랜섬웨어 생태계를 교란하고 범죄자에게 안전한 피난처를 제공하는 국가의 고립, (2) 랜섬웨어 범죄 조사 그리고 법 집행 기관 및 기타 당국을 통해 랜섬웨어 공격에 관련된 인프라와 행위자를 저지할 것, (3) 랜섬웨어 공격을 견딜 수 있도록 주요 인프라의 복원력 강화, (4) 탈취한 돈을 세탁하기 위해 가상 화폐를 악용하는 것을 방지하기 위한 조치를 취할 예정

• CISA와 FBI가 공동 의장을 맡은 랜섬웨어 대응 태스크포스(JRTF, Joint Ransomware Task Force)는 랜섬웨어 방지를 위한 부처간 노력을 조정 하고 민간 부문과 협력을 강화하도록 지원할 것

• 랜섬웨어 운영자가 이용하는 불법 암호화폐 거래소에 대한 제재와 불법 가상 자산 금융과 싸우기 위한 국제 표준 또한 개선할 예정

7 주요 인프라의 사이버보안 개선에 관한 행정명령

[표 11] NCS 전략 2.5 실행계획 주요 내용

NCS 2.5 실행계획(NCSIP)	책임기관	완료기한
2.5.1 랜섬웨어 범죄자를 위한 피난처 비활성화 (Disicentivize safe havens for ransomware criminals)	DOS (국무부)	4분기 FY23
2.5.2 랜섬웨어 범죄 근절 (Disrupt ransomware crimes)	FBI (연방수사국)	1분기 FY24
2.5.3 랜섬웨어 범죄 조사 및 랜섬웨어 생태계 파괴 (Investigate ransomware crimes and disrupt the ransomware ecosystem)	DOJ (법무부)	2분기 FY24
2.5.4 랜섬웨어 위험 완화를 위한 민간 부문 및 연방 정부 및 주 지방 (SLTT) 정부의 노력 지원 (Support private sector and state, local, Tribal, and territorial(SLTT) efforts to mitigate ransomware risk)	CISA (사이버보안,인프라 보안국)	1분기 FY25
2.5.5 가상 자산 서비스 제공업체에 대한 글로벌 자금세탁 방지(AML/CFT) 표준 채택 및 이행을 위한 타국의 노력 지원 (Support other countries dffort to adopt and implement the global anti-money laundering/countering the financing of terrorism(AML/CFT) standards for virtual asset service providers)	재무부 (DOT)	4분기 FY24

• 이니셔티브 2.5.1 : 랜섬웨어 범죄자를 위한 피난처 비활성화

- JRTF와 협력하여 법무부 및 기타 이해관계자와 협력을 통해 국가가 랜섬웨어 범죄자의 안전한 피난처 역할을 하는 것을 방지하고 다국적 사이버 범죄에 대응하기 위한 국제협력을 강화하기 위한 계획 개발 예정

• 이니셔티브 2.5.2 : 랜섬웨어 범죄 근절

- FBI는 JRTF와 협력하여 법무부, CISA 및 기타 연방 기관 등 국제 및 민간 부문 파트너와 협력하여 랜섬웨어 수익금 세탁을 가능하게 하는 자산 제공업체와 초기 액세스 자격 증명 또는 랜섬웨어 활동에 대한 기타 자료 자원을 제공하는 웹 포럼을 포함한 랜섬웨어 생태계에 대한 교란 작전을 수행할 것

• 이니셔티브 2.5.3 : 랜섬웨어 범죄 조사 및 랜섬웨어 생태계 파괴

- 법무부는 상호 법적 자원 채널과 국내 법적 절차, 몰수 절차 및 형사기소 기관을 활용하여 연방 및 국제, 민간 부문 파트너와 협력하여 랜섬웨어 생태계를 중단 및 조정할 수 있는 역량을 강화할 예정

• 이니셔티브 2.5.4 : 랜섬웨어 위험 완화를 위한 민간 부문 및 연방정부 및 주 지방 정부의 노력

- CISA는 JRTF, SRMA 및 기타 이해관계자와 협력을 통해 교육, 사이버보안 서비스, 기술 평가 등 랜섬웨어의 고위험 대상에 대한 사고 대응과 같은 리소스를 제공하여 피해 규모를 줄일 것

• **이니셔티브 2.5.5 : 가상자산 서비스 제공업체에 대한 글로벌 자금세탁 방지(AML/CFT) 표준 채택 및 이행을 위한 타국의 노력 지원**

– 재무부는 법무부, 주정부 및 정부 이해관계자들과 함께 재무부 주도의 FATF[8] 대표단을 통해 자금 세탁 방지를 위한 글로벌 채택 및 구현을 가속화하여 테러자금 조달(AML/CFT) 표준 및 가상 자산 서비스 공급자를 감독하고 랜섬웨어 수익금 세탁을 가능하게 하는 제공자를 억지할 것

1-3 보안 및 복원력 촉진을 위한 시장의 힘 형성 (Shape Market Forces To Drive Security and Resilience)

• 안전하고 복원력 있는 디지털 미래를 조성하기 위해서는 생태계 내에서 위험을 줄이는 데 가장 뛰어난 역량을 갖춘 사람들에게 책임을 부여하도록 시장의 힘을 형성하고 사용할 것

• 연방정부는 디지털 생태계의 지속적이고 장기적인 보안과 복원력 형성을 위해 데이터 관리자에게 개인 데이터 보호에 대한 책임을 강화하여 안전한 데이터 연결 장치의 개발을 촉진

• 보안 오류, 소프트웨어 취약성 및 디지털 기술로 인해 발생하는 데이터 손실과 피해에 대한 책임을 규율하는 법률을 개정

• 사이버 보안을 장려하기 위해 연방 구매력 강화와 보조금을 지급할 예정이며 이를 통해 더 나은 사이버안보 관행을 추진하고 정부가 치명적인 위험으로부터 사이버 보험 시장을 안정화 할 수 있는 방법 탐구

▮ 전략 3.1 : 데이터 관리자에 대학 책임 강화(Hold the Stewards of Our Data Accountable)

• 개인의 데이터를 보유한 기관이 데이터 보호 의무를 소홀히 하면 그 피해는 일반 국민에게 전가되고 가장 큰 피해는 개인 데이터에 대한 위험으로 인해 막대한 피해를 입을 수 있는 취약계층이 될 것

• 연방정부는 개인 데이터의 수집 및 사용 등에 대한 명확한 규제방침 수립과 보호 조치를 제공하는 입법을 통해 개인정보 보호를 위한 국가적 의무요건이 NIST에서 개발한 표준 및 지침에 부합하도록 설정할 계획

▮ 전략 3.2 : 안전한 IoT 기기의 개발 촉진(Drive The Development of Secure IoT Devices)

• IoT는 새로운 형태의 연결성을 제공하나 상당수가 사이버 위협으로부터 적절히 보호되지 못하고 있어 정부는 'IoT 사이버보안 개선법'[9]에 따라 연구개발, 위험 관리 등의 노력을 통해 지속적으로 보안을 개선할 방침

• 또한, 행정명령 14028호에 따라 'IoT 보안 라벨링 프로그램' 개발도 지속하고 확대하여 소비자는 다양한 IoT 제품의 사이버보안 기능을 비교할 수 있게 될 것

8 국제자금세탁방지기구
9 IoT Cybersecurity Improvement Act(2020)

[표 12] NCS 전략 3.2 실행계획 주요 내용

NCS 3.2 실행계획(NCSIP)	책임기관	완료기한
3.2.1 Implement Federal Acquisition Regulation(FAR) requirements per the Internet of Things(IoT) Cybersecurity Improvement Act of 2020 (2020년 사물인터넷(IoT) 사이버보안 개선법에 따라 연방 취득 규정(FAR) 요건 이행)	예산관리실 (OMB)	4분기 FY23
3.2.2 Initiate a U.S. Government IoT security labeling program (미국 정부 IoT 보안 라벨링 프로그램 시작)	국가안보회의 (NSC)	4분기 FY23

• **이니셔티브 3.2.1 : 2020년 사물인터넷 사이버보안 개선법에 따라 연방 취득 규정 요건 이행**

– OMB는 연방조달규정을 통해 의회와 협력하여 2020년 사물인터넷(IoT) 사이버보안 개선법에 따라 연방 취득 규정을 변경할 예정

• **이니셔티브 3.2.2 : 미국 정부 IoT 보안 라벨링 프로그램 시작**

– NSC는 미국 정부 사물인터넷(IoT) 보안 라벨링 프로그램의 광범위한 초안을 작성하여 이를 수행할 기관을 선별할 예정

▮ 전략 3.3 : 안전하지 않은 소프트웨어 제품 및 서비스에 대한 책임 (Shift Liability for Insecure Software Products and Services)

• 수많은 공급업체가 안전한 제품 개발을 위해 확립된 모범 사례를 무시하고 취약점이 알려진 제품을 배포하며 출처를 알 수 없는 제3의 소프트웨어를 통합하는 실정

– 소프트웨어 제작사는 소비자와 기업 등에 대한 보안 의무를 다하지 못하는 경우에 책임이 필요하며 이러한 책임은 피해를 예방할 역량을 갖춘 이해관계자들에게 초점을 맞출 것

– 연방정부는 소프트웨어 제품 및 서비스를 안전하게 개발하고 유지 관리하는 기업을 규제나 책임으로부터 보호하는 '세이프 하버(Safe harbor) 프레임워크'[10]를 구축할 예정

– 안전한 소프트웨어 개발 관행을 장려하기 위해 모든 기술 유형과 부문에 걸쳐 취약점 공개를 장려하고, SBOM의 추가 개발을 촉진해 안전하지 않은 소프트웨어로 인해 발생하는 위험을 완화할 계획

[표 13] NCS 전략 3.3 실행계획 주요 내용

NCS 3.3 실행계획(NCSIP)	책임기관	완료기한
3.3.1 Explore approaches to develop a long-term, flexible, and enduring software liability framework (장기적이고 유연하며 지속적인 소프트웨어 책임 프레임워크를 개발하기 위한 접근 탐색)	ONCD (국가사이버실)	2분기 FY24

[10] 세이프 하버 프레임 워크 : 미국과 EU간의 개인 데이터 전송 간소화 프로세스의 명칭과 같으나 이 경우에는 소프트웨어 개발과 관리 유지 책임에 대한 새로운 관리 규정을 개발한 다는 것으로 해석

NCS 3.3 실행계획(NCSIP)	책임기관	완료기한
3.3.2 Advance sofrware bill of materials(SBOM) 뭉 mitigate the risk of unsupported software (SBOM 개선 및 지원되지 않는 소프트웨어 위험을 완화)	CISA (사이버보안,인프라 보안국)	2분기 FY25
3.3.3 Coordinated vulnerability disclosure (조정된 취약점 공개)	CISA (사이버보안,인프라 보안국)	4분기 FY25

• **이니셔티브 3.3.1 : 장기적이고 유연하며 지속적인 소프트웨어 책임 프레임워크를 개발하기 위한 접근 탐색**

- ONCD는 학계 및 시민 사회의 이해관계자와 협력하여 다양한 규제법 영역에서 끌어온 소프트웨어 책임 프레임워크에 대한 다양한 접근 방식을 탐구하고 소프트웨어 프레임워크에 대한 다양한 의견 수렴을 위해 컴퓨터 과학자의 의견을 반영하는 법적 심포지엄을 개최할 예정

• **이니셔티브 3.3.2 : SBOM 개선 및 지원되지 않는 소프트웨어의 위험 완화**

- 중요 인프라에서 호환 불가한 소프트웨어 사용에 대한 데이터를 수집하기 위해 CISA는 SRMA를 포함한 주요 이해관계자와 협력하여 SBOM 규모 및 구현의 격차를 식별하여 해소할 것
- 또한 CISA는 수명 종료 및 지원이 종료된 소프트웨어에 대해 세계적으로 액세스할 수 있는 데이터베이스에 대한 요구 사항을 연구하여 SBOM에 대한 국제적인 규모의 워킹 그룹을 소집할 예정

• **이니셔티브 3.3.3 : 조정된 취약점 공개**

- CISA는 국제 취약성 조정자 실무 커뮤니티 생성을 포함하여 모든 기술 유형 및 분야에 걸쳐 공공 · 민간 기관 간에 조정된 취약성 공개에 대해 국내 및 국제 지원을 구축하기 위해 노력할 것

▮ 전략 3.4 : 보안 강화를 위한 연방 보조금 및 기타 인센티브 부여 (Use Federal Grants and Other Incentives to Build In Security)

• 연방 보조금 프로그램은 사이버안보 및 모든 위험에 대한 복원력을 염두에 두고 설계, 배치, 개발, 유지관리 중인 주요 인프라에 투자할 수 있는 전략적 기회를 제공

- 연방정부는 “초당적 인프라법”, “인프레이션 감축법”, “반도체 생산지원 및 과학법”이 지원하는 보조금 프로그램을 통해 각 분야 인프라를 지원하는 막대한 규모의 투자를 진행 중
- 중요 인프라 사이버안보 및 회복탄력성 개선에 초점을 맞춘 사이버안보 연구개발 및 시연(RD&D) 프로그램에 우선순위를 두고 자금을 지원할 예정

[표 14] NCS 전략 3.4 실행계획 주요 내용

NCS 3.4 실행계획(NCSIP)	책임기관	완료기한
3.4.1 기반시설 사이버보안 개선을 위한 연방 보조금 활용 (Leverage Federal grants to improve infrastructure cybersecurity)	ONCD (국가사이버실)	4분기 FY23
3.4.2 사이버 보안 연구를 위한 자금 우선 배정 (Prioritize funding for cybersecurity research)	OSTP (과학기술정책국)	4분기 FY23

NCS 3.4 실행계획(NCSIP)	책임기관	완료기한
3.4.3 사이버 보안의 사회, 행동 및 경제 연구에 대한 사이버 보안 연구, 개발 및 시연의 우선 순위화 (Prioritize cybersecurity research, development, and demonstration on social, behavioral, and economic research in cybersecurity)	NSF (국립과학재단)	4분기 FY24

• **이니셔티브 3.4.1 : 기반시설 사이버보안 개선을 위한 연방 보조금 활용**

- ONCD는 사이버보안 자산을 연방 보조금 프로젝트에 통합하기 위한 자료를 개발할 예정

• **이니셔티브 3.4.2 : 사이버보안 연구를 위한 자금 우선 배정**

- OSTP는 ONCD 및 OMB와 협력하여 2025 회계연도 예산 프로세스를 통해 중요 인프라의 보안 및 복원력 강화를 목표로 하는 사이버보안 연구, 개발 및 시연의 우선순위를 확립할 것

• **이니셔티브 3.4.3 : 사이버보안의 사회, 행동 및 경제 연구에 대한 사이버보안 연구, 개발 및 시연의 우선 순위화**

- NSF는 사이버 경제, 인적 요소, 정보 무결성 및 관련 주제에 대한 연구를 통해 사이버보안에 대한 개인 및 사회적 영향과 사이버보안이 개인 및 사회에 미치는 영향에 대한 이해를 높이는데 투자할 것

▮ 전략 3.5 : 연방정부의 조달을 활용한 책임 강화 (Leverage Federal Procurement to Improve Accountability)

• 행정명령 14028은 공급망 보안에 대한 계약 요건이 연방 기관 전체에 걸쳐 강화되도록 하여 조달을 통해 사이버안보 요건을 수립 및 시행하기 위한 개념을 시범적으로 적용하여 혁신적인 접근 방식을 개발할 수 있게함

- 연방정부와 계약 시 보안 모범 사례를 따른다는 계약을 준수해야 하며 민간 사이버 사기 이니셔티브 및 “허위 주장법”에 따라 법무부는 보안 의무를 이행하지 않는 정부 보조금 및 계약자에 대한 민사 소송을 진행

[표 15] NCS 전략 3.5 실행계획 주요 내용

NCS 3.5 실행계획(NCSIP)	책임기관	완료기한
3.5.1 행정명령 14028에 따라 요구되는 FAR 변경 요구사항 구현 (Implement Federal Acquisiton Regulation(FAR) changes required under EO14028)	OMB (예산관리실)	1분기 FY24
3.5.2 공급업체 사이버보안 개선을 위해 부정 청구법 활용 (Leverage the False Claims Act to improve vendor cybersecurity)	DOJ (법무부)	4분기 FY25

• **이니셔티브 3.5.1 : 행정명령 14028에 따라 요구되는 FAR(연방조달규정) 변경 요구사항 구현**

- OMB는 연방조달규제위원회와 협력하여 행정명령 14028에 따라 요구되는 FAR에 대한 변경사항 수립

- 초안(사이버보안 사건 보고, 사이버보안 계약 요구사항 표준화 등) 공개를 통해 변경사항을 확정하기 전에 대중들의 의견을 고려하여 반영할 것

• **이니셔티브 3.5.2 : 공급업체 사이버보안 개선을 위해 부정 청구법 활용**

- 법무부는 복원력 구축, 취약성 공개 증가, 책임있는 공급업체의 불이익 감소, 연방 프로그램 및 기관의 피해복구를 목적으로 연방 계약 및 보조금 부문에서 사이버보안 요구 사항을 미준수 기업을 식별, 추적, 방지하기 위한 노력을 확대할 예정

▮ 전략 3.6 : 연방정부 차원의 사이버 보험 지원 방안 설계 (Explore A Federal Cyber Insurance Backstop)

• 연방정부는 중대한 사이버 사건에 대해 연방 사이버 보험의 필요성과 실현 가능성에 대해 평가하고 의회, 주 규제 기관 및 산업계로부터 의견을 구하고 협의를 진행할 예정

[표 16] NCS 전략 3.6 실행계획 주요 내용

NCS 3.6 실행계획(NCSIP)	책임기관	완료기한
3.6.1 심각한 사이버 사건에 대한 연방 보험 대응의 필요성 평가 (Assess the need for a Federal insurance response to a catastrophic cyber event)	DOT (재무부)	1분기 FY24

• 이니셔티브 3.6.1 : 심각한 사이버 사건에 대한 연방 보험 대응의 필요성 평가

– 재무부는 CISA 및 OMD와 협력하여 기존 사이버 보험 시장을 지원하는 치명적인 사이버 사건에 대한 연방 보험 대응의 필요성을 평가할 것

1-4 복원력 있는 미래에 투자(Invest In a Resilient Future)

• 차세대 디지털 인프라를 구축하고 인공지능 및 양자 컴퓨팅이 가져올 기술 환경의 혁신적인 변화에 대비하면서 투자 격차를 해소해야 함

• 연방정부는 R&D 및 교육에 대한 전략적 공공 투자와 안전하고 신뢰할 수 있는 사이버 공간 프로그램을 활용하여 기술 및 혁신 분야에서 미국의 지속적인 리더십을 유지할 것

• 악의적 행위자들로 인해 사이버보안 없이 디지털 기술 혁신을 주도하는 것은 불가능하며 사이버보안 기술의 개발 및 배포를 위해 집중적인 노력을 다할 것

▮ 전략 4.1 : 인터넷 구성 기술의 안전한 기반 확보 (Secure the Technical Foundation of the Internet)

• 시스템 전체의 위험을 완화하기 위해 가장 시급한 보안 문제를 파악하여 보안 조치를 추가로 개발하며, 이러한 인프라 위에 구축된 플랫폼과 서비스가 중단되지 않고 위험 노출을 줄이기 위한 민 · 관 협력이 필요

• 연방정부는 비정부 표준개발기구(SDO, Standards Developing Organization)에 대한 지원을 통해 다양한 분야와 협력을 통해 신기술을 확보하여 국가 안보와 경제적 이점을 보호할 것

[표 17] NCS 전략 4.1 실행계획 주요 내용

NCS 4.1 실행계획(NCSIP)	책임기관	완료기한
4.1.1 네트워크 보안 모범 사례 채택 주도 (Lead the adoption of network security best practices)	OMB (예산관리실)	2분기 FY24
4.1.2 오픈 소스 소프트웨어 보안 및 메모리 안전 프로그래밍 언어 채택 촉진 (Promote open-source software security and the adoption of memory safe programming languages)	ONCD (국가사이버실)	1분기 FY24
4.1.3 기본적인 인터넷 인프라 기능 및 기술의 개발, 표준화 및 채택 가속화 (Accelerate development, standardization, and adoption of foundational Internet infrastructure capabilities and technologies)	NIST (국립표준기술연구소)	1분기 FY24
4.1.4 기본적인 인터넷 인프라 기능 및 기술의 개발, 표준화 및 채택 지원 가속화 (Accelerate development, standardization, and adoption of foundational Internet infrastructure capabilities and technologies)	NIST (국립표준기술연구소)	4분기 FY24
4.1.5 안전한 인터넷 라우팅 확산을 위한 핵심 이해관계자와 협력 (Collaborate with key stakeholders to drive secure Internet routing)	ONCD (국가사이버실)	3분기 FY24

• 이니셔티브 4.1.1 : 네트워크 보안 모범 사례 채택 촉진

- OMB는 CISA 및 연방기관과 협력하여 제로트러스트 전략 및 성숙도 모델(M-22-09)에 따라 도메인 시스템 요청 시, 암호화 우선순위를 설정

• 이니셔티브 4.1.2 : 오픈 소스 소프트웨어 보안 및 메모리 안전 프로그래밍 언어 채택 촉진

- ONCD는 OS3I[11]를 수립하여 메모리 안전 프로그래밍 언어와 오픈 소스 소프트웨어 보안의 채택을 장려
- 이 전략 실행계획의 일환으로 CISA는 OS3I 및 오픈 소스 소프트웨어 커뮤니티와 협력하여 연방정부 및 중요 인프라에서 오픈 소스 소프트웨어를 안전하게 사용하도록 권고하며 소프트웨어 에코시스템의 보안 기준을 제고할 예정

• 이니셔티브 4.1.3 : 기본적인 인터넷 인프라 기능 및 기술의 개발과 표준화 및 채택 지원 가속화

- 국가 표준 전략에 따라 NIST는 기관 간 국제 사이버보안 표준화 작업 그룹을 소집하여 국제 사이버보안 표준화의 주요 문제를 조정하고 미국 연방기관의 프로세스 참여를 강화할 것

• 이니셔티브 4.1.4 : 기본적인 인터넷 인프라 기능 및 기술의 개발, 표준화 채택 지원 가속화

- NIST는 국제 표준의 개발, 상용화 및 채택을 추진하여 BGP[12] 및 IPv6[13] 보안 격차를 해결하기 위해 기관, 산업, 학계 및 기타 커뮤니티와 협력할 예정

11 Open source software security Initiative
12 Border Gateway Protocol
13 Internet Protocol Version 6

• **이니셔티브 4.1.5 : 안전한 인터넷 라우팅 확산을 위한 핵심 이해관계자와 협력**

- ONCD는 주요 이해관계자 및 연방정부 기관과 함께 안전한 인터넷 라우팅 기술 채택을 늘리기 위한 로드맵을 개발할 것
- △ 인터넷 라우팅 및 BGP 보안 문제를 해결하기 위한 접근방식과 옵션 탐색, △ 모범 사례의 개발 및 식별, △ 필수적인 연구 및 개발 사안 조사, △ 기술 채택에 대한 규제완화 방법 모색

▮ 전략 4.2 : Cybersecurity를 위한 연방 연구 및 개발 활성화 (Reinvigorate Federal Research and Development for Cybersecurity)

• 연방정부의 주요 조직을 통해 연구개발 및 시연(RD&D) 프로젝트를 촉진하여 인공지능, 클라우드 등 주요 인프라에서 사용되는 데이터 분석과 같은 영역의 사이버안보 및 복원력을 향상 시킬 것

• R&D 투자는 향후 10년간 미국에 필수적인 기술군인 마이크로 일렉트로닉스, 양자 정보 시스템, 인공지능 컴퓨팅 기술, 생명공학 및 바이오 제조, 청정에너지 기술 확보에 집중

• 연방 투자 수단, 구매력 및 규제를 활용하여, 조율된 전략적 혁신을 촉진하고 신뢰할 수 있는 제품 및 서비스 시장을 창출하는 것을 목표로 하는 광범위한 산업 및 혁신 전략을 지원할 예정

[표 18] NCS 전략 4.2 실행계획 주요 내용

NCS 4.2 실행계획(NCSIP)	책임기관	완료기한
4.2.1 메모리 안전 프로그래밍 언어의 완성도, 채택 및 보안 가속화 (Accelerate maturity, adoption, and security of memory safe programming languages)	OSTP (과학기술정책국)	1분기 FY24

• **이니셔티브 4.2.1 : 메모리 안전 프로그래밍 언어의 완성도, 채택 및 보안 가속화**

- 연방 사이버보안 R&D 전략 계획을 통해 OSTP는 NSF, NIST, 보조금 지급 기관, OS3I 및 기타 관련 연방 파트너와 협력하여 애플리케이션, 운영 체제 및 중요 인프라에서 메모리 안전 프로그래밍 언어의 성숙도, 채택 및 보안을 가속화하기 위한 투자의 우선순위 설정

▮ 전략 4.3 : 포스트 양자 암호를 위한 준비 (Prepare for Our Post-Quantum Future)

• 강력한 암호화는 사이버안보에서 매우 중요한 요소이나 양자 컴퓨팅은 현대의 암호화 표준을 깨트릴 잠재력을 가지고 있어 미래의 공격에 대비하기 위해 양자 컴퓨터에 대한 투자를 가속화 해야함

• 양자 컴퓨팅의 발달과 디지털 시스템에 제기되는 위협의 균형을 맞추기 위해 “국가안보각서 10호”에 따라 국가의 암호화 시스템을 상호 운용 가능한 상태로 적시에 전환하는 프로세스를 수립할 예정

[표 19] NCS 전략 4.3 실행계획 주요 내용

NCS 4.3 실행계획(NCSIP)	책임기관	완료기한
4.3.1 국가안보각서(NSM)-10 이행 (Implement National Security Memorandum-10)	OMB (예산관리실)	1분기 FY25
4.3.2 NSS용 NSM-10 구현 (Implement NSM-10 for National Security Systems (NSS))	NSA (국가안보국)	3분기 FY25
4.3.3 포스트 양자 암호화 알고리즘 표준화 및 전환 지원 (Standardize, and support transition to, post-quantum cryptographic algorithms)	NIST (국립표준기술연구소)	1분기 FY25

• **이니셔티브 4.3.1 : 국가안보각서(NSM-10) 이행**

- OMB와 연방기관의 보안 시스템 관리자는 ONCD와 협력하여 NSM-10의 구현과 취약한 공용 네트워크 및 시스템을 양자 저항 암호화 기반 환경으로 전환하는 우선순위를 설정할 것
- OMB는 NIST와 협력을 바탕으로 암호화 민첩성을 제공하는 보완적인 완화 전략을 개발할 예정

• **이니셔티브 4.3.2 : NSS용 NSM-10 구현**

- NSS(국가보안시스템)를 양자 저항 암호화 체계로 전환

• **이니셔티브 4.3.3 : 포스트 양자 암호화 알고리즘 표준화 및 전환 지원**

- NIST는 하나 이상의 양자 저항 공개 키 암호화 알고리즘을 표준화하는 프로세스를 완성하고 이를 통해 새로운 공개 키 암호화 표준을 전 세계적으로 사용 가능하도록 지원하여 민감한 정부 정보를 보호할 것

▮ 전략 4.4 : 청정 에너지 미래 확보(Secure Our Clean Energy Future)

• 청정 에너지 미래로 국가적 전환이 가속화되면서 미국 전력망의 복원력과 안전, 효율성을 개선할 수 있는 새로운 상호 연결 시스템이 도입되고 있으며 디지털 방식으로 자동화되고 있음

- 연방정부는 사후적 보안 제어를 추가하기보다는 국가 사이버 기반 엔지니어링 전략의 이행을 바탕으로 사전에 구축할 수 있는 전략적 기회를 포착할 것
- 에너지부는 업계, 주, 연방 규제 기관 등과 협력하여 에너지 자원에 대한 보안을 강화할 예정

[표 20] NCS 전략 4.4 실행계획 주요 내용

NCS 4.4 실행계획(NCSIP)	책임기관	완료기한
4.4.1 사이버 보안 설계 원칙을 연방 프로젝트에 통합하여 채택 촉진 (Drive adoption of cyber secure-by-design principles by incorporating them into Federal projects)	DOE (에너지부)	1분기 FY24
4.4.2 디지털 생태계가 미국 정부의 탈탄소 목표를 지원하고 제공할 수 있도록 보장하는 계획 개발 (Develop a plan to ensure the digital ecosystem can support and deliver the U.S. government's decarbonization goals)	ONCD (국가사이버실)	2분기 FY24

NCS 4.4 실행계획(NCSIP)	책임기관	완료기한
4.4.3 사이버 정보 엔지니어링 원칙을 토대로 엔지니어와 기술자를 위한 교육, 도구, 지원안 구축 및 개선 (Build and refine training, tools, and support for engineers and technicians using cyber-informed engineering principles)	DOE (에너지부)	4분기 FY25

• 이니셔티브 4.4.1 : 사이버보안 설계 원칙을 연방 프로젝트에 통합하여 채택 촉진

- 에너지부는 ONCD 및 CISA, 이해관계자와 협력하여 사이버보안 설계 시범 프로젝트를 구현하고 사이버 설계를 위한 경제적 인센티브와 사이버 설계 원칙 적용에 필요한 기술을 파악하여 사이버보안 설계에 구현을 위한 전략을 실행할 것

• 이니셔티브 4.4.2 : 디지털 생태계가 미국 정부의 탈탄소 목표를 지원하고 제공할 수 있도록 보장하는 계획 개발

- 에너지부와 ONCD는 디지털 생태계가 청정에너지 전환을 지원하는 데 필요한 새로운 기술과 역학을 통합하기 위한 계획을 개발할 것
- 해당 계획은 미국 정부 전반의 기존 정책들을 이어가며 우선순위에 대한 격차 및 요구사항 파악, 반도체 생산에 유용한 인센티브 개발 등 국가의 투자가 사이버보안을 유지하고 설계에 따라 탄력적으로 청정에너지 생태계의 새로운 운영 환경을 지원할 수 있도록 할 것

• 이니셔티브 4.4.3 : 사이버 정보 엔지니어링 원칙을 토대로 엔지니어와 기술자를 위한 교육, 도구 지원 방안 구축 및 개선

- 에너지부는 이해관계자와 협력하여 엔지니어와 기술자가 안전하고 탄력적으로 구축 및 운영 기술과 제어 시스템을 설계하여 운영할 수 있도록 교육하고 활용 가능한 도구를 발전시키는 전략을 구축할 것

▮ 전략 4.5 : 디지털 ID 생태계 개발 지원(Support Development of a Digital Identity Ecosyste)

• 신원 도용이 증가하고 있으며 동의를 원칙으로 한 디지털 신원 솔루션이 부재한 상황에서 사이버 범죄가 증폭하고 금융 활동 등과 같은 일상생활에서 비효율을 초래하고 있음

• 연방정부는 보안, 접근성, 상호운용성, 개인정보 보호 등 경제 성장을 촉진하는 강력한 디지털 신원 솔루션에 대한 투자를 장려할 예정

- NIST의 디지털 신원 연구 프로그램에는 디지털 자격 증명의 보안 강화, 자격 증명 검증 서비스 제공, 투명성을 강조하는 디지털 신원 플랫폼 개발 등이 포함
- 디지털 ID 정책과 기술 개발 시 개인 프라이버시, 시민의 자유를 보호하고 잠재적 오용을 방지하며 사용자가 공급업체를 선택하고 자발적으로 기술을 사용할 수 있도록 지원 예정

▮ 전략 4.6 : 사이버 인재 육성을 위한 국가 전략 개발 (Develop a National Strategy to Strengthen Our Cyber Workforce)

- 사이버보안 인력은 매우 부족하며 민간과 공공 모두 인력 채용 및 고용유지에 어려움을 겪고 있어 이 같은 현상은 국가 사이버안보에 부정적인 영향을 미치고 있음

- 주요 인프라에 중점을 두고 모든 부문에서 사이버안보 전문 지식의 필요성을 강조하여 미국의 인재들이 복원력 있는 차세대 사이버보안 기술을 계속해서 개발할 수 있도록 지원할 예정

- 국립과학재단(NSF, National Science Foundation) 및 기타 기관에서 진행하는 다양한 인력 개발 프로그램을 활용하여 연방 정부 보안 인력 양성 프로그램[14]을 강화할 계획

[표 21] NCS 전략 4.6 실행계획 주요 내용

NCS 4.6 실행계획(NCSIP)	책임기관	완료기한
4.6.1 국가 사이버 인력 및 교육 전략 게시 및 구현 추적 (Publish a National Cyber Workforce and Education Strategy and track its implementation)	ONCD (국가사이버실)	2분기 FY24

- **이니셔티브 4.6.1 : 국가 사이버 인력 및 교육 전략 게시 및 구현 추적**

- ONCD는 국가 사이버 인력 및 교육 전략의 개발을 주도하고 전략 구현의 초기 단계를 추진 및 조정할 예정

1-5 공동의 목표를 추구하기 위한 국제 파트너십 구축 (Forge International Partnership To Pursue Shared Goals)

- 사이버 공간에서 모든 국가가 책임 있는 행동을 하기를 기대하며 안전한 인터넷을 유지하기 위해 광범위한 국가 연합을 구축하는 동시에 공동의 문제에 대한 미국의 의제에 반대하는 국가들과도 협력하겠다고 밝힘

- 연방정부는 수십 년간 국제기구를 통해 사이버 공간에서 국가의 책임 있는 행동을 정의하고 촉진함

- UN 정부 전문가 그룹 및 개방형 실무 그룹과 같은 다양한 절차를 활용하여 모든 UN 회원국이 UN 총회에서 지지한 평시 규범과 신뢰 구축 조치를 포함하는 프레임워크를 수립함

- 사이버 범죄에 관한 부다페스트 협약의 확대와 사이버 공간의 안보를 강화하기 위한 기타 글로벌 노력을 장려하여 국가 행동 규범을 위반하는 행위에 처벌을 공동으로 시행할 것

- 보다 본질적으로 복원력이 있고 안전한 공동의 디지털 생태계로 나아가기 위해, 사이버안보 이해관계자 간의 새로운 협력 모델을 확대해 국제 사회와의 협력을 추진할 방침

- 국제 동맹국 및 파트너의 역량을 개선하고 국제법의 적용을 강화할 예정이며 평시에 책임 있는 국가 행동에 대해 국제적으로 수용가능하고 자발적인 규범을 장려할 계획

14 국가 사이버안보 교육 이니셔티브(NICE, National Initiative for Cybersecurity Education), CyberCorps Scholarship for Service 프로그램, National Centers of Academic Excellence in Cybersecurity 프로그램, Cybersecurity Education Training and Assistance Program, 각종 실습 프로그램 등

▮ 전략 5.1 : 디지털 생태계에 위협 대응을 위한 연합 구축 (Build Coalitions to Counter Threats to Our Digital Ecosystem)

• 미국과 60개 국가는 "인터넷의 미래를 위한 선언(DFI)"[15]을 통해 개방적이고 자유로운 네트워크에 대한 비전을 공유할 수 있는 최대 규모의 글로벌 파트너 연합 결성('22.4.)

- 미국 · 인도 · 일본 · 호주로 구성된 4개국 안보 회담(Quad)를 통해 사이버 공간에 대한 공동의 목표를 발전시키고 있고 IPEP[16]와 APEP[17]를 통해 디지털 경제를 위한 규정 수립을 위해 협력 중에 있음
- 미국-EU 무역 및 기술 위원회(TTC, U.S-EU Trade and Technology Council)를 통해 유럽과 협력체계를 구축했으며 호주 및 영국과도 3자 안보협력체(AUKUS)를 통해 긴밀히 협력중
- 새롭게 등장하는 사이버안보 문제를 해결하기 위한 목적으로 이해 관계자들을 소집하기 위해, 필요에 따라 국제 랜섬웨어 대응 이니셔티브처럼 새롭고 혁신적인 파트너십의 구축을 지원할 계획
- 연방정부의 디지털 시대를 위한 새로운 협력 법 집행 메커니즘을 개발하기 위해 동맹국 및 파트너와 협력할 것이며 다른 지역의 파트너와 효과적인 허브를 구축하기 위한 노력을 지원할 것

[표 22] NCS 전략 5.1 실행계획 주요 내용

NCS 5.1 실행계획(NCSIP)	책임기관	완료기한
5.1.1 지역별 사이버 협업 및 조정을 위한 기관 간 합동 팀 구축 (Create interagency teams for regional cyber collaboration and coordination)	DOS (국무부)	1분기 FY25
5.1.2 국제 사이버 공간 및 디지털 정책 전략 공개 (Publish an International Cyberspace and Digital Policy Strategy)	DOS (국무부)	1분기 FY24
5.1.3 동맹 및 협력 파트너와의 연방 법 집행 기구 협업 메커니즘 강화 (Strengthen Federal law enforcement collaboration mechanisms with allies and partners)	FBI (연방수사국)	4분기 FY25
5.1.4 지역 사이버 허브 연구 (Regional cyber hubs study)	ONCD (국가사이버실)	4분기 FY24

• 이니셔티브 5.1.1 : 지역별 사이버 협업 및 조정을 위한 기관 간 합동 팀 구축

- 국무부는 파트너 국가와의 협력을 용이하게 하기 위해 국가 및 지역 간 사이버 팀을 구축하고 강화할 예정이며 디지털 정책과 관련된 부서 직원의 역량과 기술을 개발할 것

15 DFI(Declaration for the Future of the Internet) - 미국, EU, 호주, 영국, 일본, 캐나다, 일본 등 60개국이 참여하여 자유로운 인터넷과 디지털 기술의 비정치적 비전을 제시하고 디지털 독재에 대응하는 인터넷 거버넌스를 위한 선언으로 한국은 당시 참여하지 않음

16 인도-태평양 경제 프레임워크(Indo-Pacific Economic Framework for Prosperity)

17 경제 번영을 위한 미주 파트너십(Americas Partnership for Economic Prosperity)

• **이니셔티브 5.1.2 : 국제 사이버 공간 및 디지털 정책 전략 공개**

– 2023 회계연도 국방수권법에 따라 국무부는 양자 및 다자간 활동을 통합하기 위한 국제 사이버 공간 및 디지털 정책 전략을 발표할 예정

• **이니셔티브 5.1.3 : 동맹 및 협력 파트너와의 연방 법 집행기구 협업 메커니즘 강화**

– FBI는 사이버 범죄자, 국가적 적대자, 관련 조력자들에 대한 국제 법 집행 중단 캠페인의 규모와 속도를 높이기 위해 동맹국 및 파트너와의 조정을 보장하는 메커니즘을 개발하고 확장할 것

• **이니셔티브 5.1.4 : 지역 사이버 허브 연구**

– ONCD는 유럽 사이버 범죄 센터에 대한 연구를 의뢰하고 미래의 사이버 허브 개발에 정보를 제공받을 예정

▮ 전략 5.2 : 국제 파트너의 역량 강화(Strengthen International Partner Capacity)

• 미국은 공동의 사이버안보를 발전시키고 디지털 생태계에 대한 공동의 비전과 목표를 지원하기 위해 전 세계적으로 같은 비전을 가진 파트너들과 동맹국으로서 역량을 강화할 것

– 법무부(DOJ)는 양 · 다자간 참여 및 협정, 공식 · 비공식 협력을 통해 보다 강력한 사이버 범죄 협력 패러다임을 구축하고 사이버 범죄 법률, 정책 및 운영을 강화하기 위한 리더십을 제공할 예정

– 국방부(DOD)는 미국의 집단적 사이버안보 태세에 기여할 수 있는 역량을 구축하는 동시에 동맹국과 파트너의 고유한 기술과 관점을 활용하기 위한 군대 간 협력 관계를 강화할 것

– 국무부(DOS)는 연방의 역량 구축 순위를 전략적으로 조정하고 동맹국 및 파트너의 이익이 증진되도록 정부의 노력을 계속 조율 할 계획

[표 23] NCS 전략 5.2 실행계획 주요 내용

NCS 5.2 실행계획(NCSIP)	책임기관	완료기한
5.2.1 국제 파트너와의 사이버 역량 강화 (Strengthen international partners' cyber capacity)	DOS (국무부)	1분기 FY24
5.2.2 법 집행 협력을 통한 국제 파트너와의 사이버 역량 확대 (Expand internaational partners' cyber capacity through operational law enforcement collaboration)	DOJ (법무부)	4분기 FY26

• **이니셔티브 5.2.1 : 국제 파트너와의 사이버 역량 강화**

– 국무부 및 이해관계자들은 사이버 역량 구축을 위한 실무 그룹을 활용하여 사이버 공간의 글로벌 정책 동향을 평가하고 정부기관 커뮤니티와 함께 해당 전략의 진행 상황과 투자여부를 검토할 것

• **이니셔티브 5.2.2 : 법 집행 협력을 통한 국제 파트너와의 사이버 역량 확대**

– 연방법 집행 기관은 국제 파트너와 협력을 강화를 토대로 미국 법 집행 기관의 목표와 일치하는 속도와 규모로 사이버 위협을 억제할 수 있는 파트너의 역량을 강화할

▮ 전략 5.3 : 동맹국 및 파트너를 지원하기 위한 미국의 역량 강화 (Expand U.S. Ability to Assist Allies and Partners)

• 최근 코스타리카, 알바니아, 몬테네그로에 대한 사이버 공격 사례에서 알 수 있듯 동맹국과 파트너는 사건의 대응 및 복구를 위해 미국에 지원 요청을 할 수 있음

– 동맹국 및 파트너에 지원을 제공하는 것은 미국의 외교 정책과 사이버안보 목표 향상에도 도움이 되며 적에게 동맹국의 연대와 권위를 보임으로 위협에 대한 책임을 부과하기 위한 노력 가속화에 도움이 됨

– 연방정부는 지원 제공을 위해 재정적, 절차적 장애 요인 등을 제거하고 가장 국익에 부합하는 시기 등을 조율하기 위한 정책을 수립할 계획

[표 24] NCS 전략 5.3 실행계획 주요 내용

NCS 5.3 실행계획(NCSIP)	책임기관	완료기한
5.3.1 신속한 사이버 사고 대응 지원을 제공하기 위한 유연한 해외원조 체계 구축 (Establish flexible foreign assistance mechanisms to provide cyber incident response support quickly)	DOS (국무부)	1분기 FY24

• 이니셔티브 5.3.1 : 신속한 사이버 사고 대응 지원을 제공하기 위한 유연한 해외원조 체계 구축

– 국무부는 사이버 사고 대응 지원을 제공하기 위해 유연하고 신속한 해외 지원 메커니즘을 식별 및 개발할 예정

▮ 전략 5.4 : 책임있는 구가 행동 규범의 전 세계적 이행을 강화하기 위한 협력 체계 구축 (Build Coalitions to Reinforce Global Norms of Responsible State Behavior)

• UN 회원국은 국제법 의무사항으로 상대국의 주요한 인프라를 의도적으로 손상시키는 사이버 작전을 삼가는 것을 포함하여 사이버 공간에서 책임 있는 국가 행동의 평시 규범을 지지하는 정치적 약속에 서약함

• 미국은 약속을 이행하지 않은 국가에 위반의 책임을 물을 방침이며 미국의 동맹국 및 파트너와 협력해 비난 성명을 발표하고 결과에 대해 유의미한 책임을 부여할 것을 밝힘

[표 25] NCS 전략 5.4 실행계획 주요 내용

NCS 5.4 실행계획(NCSIP)	책임기관	완료기한
5.4.1 약속을 이행하지 못하는 국가에 책임을 부여 (Hold irresponsible states accountable when they fail to uphold their commitments)	DOS (국무부)	4분기 FY25

• 이니셔티브 5.4.1 : 약속을 이행하지 못하는 국가에 책임을 부여

– 국무부는 개방형 실무 그룹을 통해 사이버 공간에서 책임있는 국가 행동의 틀을 발전시키고 악의적 행위자에게 책임을 물을 의지가 있는 국가 연합을 강화할 것

▮ 전략 5.5 : 정보, 통신, 운영 기술 제품 및 서비스의 글로벌 공급망 안전 확보 (Secure Global Supply Chains for Information, Communications, And Operational Technology Products and Services)

- 미국 경제는 정보, 통신, 운영 기술 제품 및 서비스를 제공하는 글로벌 공급망에 의존하고 있으나 신뢰할 수 없는 해외 공급업체에 주요 제품과 서비스를 의존하는 것은 디지털 생태계의 위험을 초래
- 공급망 위험을 완화하기 위해서는 정부와 민간 부문의 전략적, 장기적 협력이 필요하고 또한, 글로벌 공급망의 균형을 재조정하고 투명성, 복원력 등을 강화해야함

– 연방정부는 5G 보안을 위한 국가 전략을 기반으로 개방형 RAN 및 공급업체 다변화 협력 이니셔티브를 통해 5G 및 차세대 무선 네트워크를 위한 안전한 공급망을 개발하기 위해 미국의 파트너와 협력하고 있음[18]

– "초당적 인프라법"을 통해 디지털 인프라 및 연방 지원 사업에 미국산 구매를 의무화 하고 있고 미국 공급망에 관한 행정명령 14017호와 반도체 생산지원 및 과학법, 인플레이션 감축법을 토대로 미국 및 미국의 파트너가 중요 제품을 생산하도록 제조업 공급망 확보를 위해 노력할 것

– 인도-태평양 경제 프레임워크, 쿼드 크리티컬 및 신기술 워킹그룹, 미국-EU 무역 기술위원회와 같은 파트너와 협력으로 공급망 위험 관리의 모범 사례를 구현하여 안전한 공급을 위한 노력을 지속할 예정

[표 26] NCS 전략 5.5 실행계획 주요 내용

NCS 5.5 실행계획(NCSIP)	책임기관	완료기한
5.5.1 안전하고 신뢰할 수 있는 ICT 네트워크 및 서비스 개발 촉진 (Promote the development of secure and trustworthy information and communication technology (ICT) networks and services)	DOS (국무부)	2분기 FY24
5.5.2 다양하고 신뢰할 수 있는 ICT 공급업체 공급망 촉진 (Promote a more diverse and resilient supply chain of trustworthy information and communication (ICT) vendors)	DOS (국무부)	2분기 FY24
5.5.3 공공 무선 공급망 혁신 기금 관리 착수 (Begin administering the Public Wireless Supply Chain Innovation Fund (PWSCIF))	NTIA (국가통신정보청)	4분기 FY23
5.5.4 핵심 인프라 부문 내외부에서 사이버 보안 공급망 위험 관리 핵심 사례의 확산 및 공표 (Promulgate and amplify Cybersecurity Supply Chain Risk Management (CSCRM) key practices across and within critical infrastructure sectors)	NIST (국립표준기술연구소)	2분기 FY25

[18] 오픈랜(Open RAN, Open Radio Access Networks)를 포함한 무선 네트워크와 공급자를 다양화하기 위한 협력 이니셔티브를 통해 Open RAN 구현의 국방부 테스트와 상호 운용 가능한 개방형 표준 기반 네트워크의 개발 및 채택을 촉진하기 위한 전기통신 및 정보청의 작업 등

• **이니셔티브 5.5.1 : 안전하고 신뢰할 수 있는 ICT 네트워크 및 서비스 개발 촉진**

- 국무부는 안전한 ICT 생태계를 위한 정책 및 규제 프레임워크의 국제적 채택을 촉진하기 위해 국제 기술 보안 및 혁신 기금을 통해 동맹국, 파트너와 협력할 것

• **이니셔티브 5.5.2 : 다양하고 신뢰할 수 있는 ICT 공급업체 공급망 촉진**

- 국무부는 개방적이고 상호 운용 가능한 네트워크 아키텍처의 개발 및 배포를 촉진하기 위해 국제 기술 보안 및 혁신 기금을 통해 동맹국, 파트너와 협력할 것

• **이니셔티브 5.5.3 : 공공 무선 공급망 혁신 기금 관리 착수**

- NTIA는 10년 간 15억 달러 규모의 공공 무선 공급망 혁신 기금을 관리하여 개방적이고 상호 운용 가능한 표준 기반 네트워크의 개발을 채택하고 촉진할 것

• **이니셔티브 5.5.4 : 핵심 인프라 부문 내외부에서 사이버보안 공급망 위험 관리 핵심 사례의 확산 및 공표**

- 소프트웨어 공급망 보안, 국가 사이버보안 우수 센터 개발 프로젝트를 통해 국내외 C-SCRM 모범 사례를 널리 알리고 확대하여 해외 공급업체에 대한 신뢰 제고

1-6 전략의 구현 방안(Implementation)

• 연방정부는 해당 전략의 목표를 달성하기 위해 국가사이버실(ONCD)은 국가안보회의(NSC)의 감독 하에 예산관리실(OMB)과 협력해 전략의 구현을 주도할 것

- 이 전략을 실행하기 위해 기존 정책을 검토하거나 새로운 정책을 만들어야 하는 경우 “국가 안보 위원회 시스템의 개선에 관한 국가안보각서 2호”에 설명된 절차를 통해 국가안보회의(NSC)가 모든 과정을 주도

• (유효성 평가) 국가사이버실은 국가안보회의, 예산관리실, 정부 부처 등과 협력해 이 전략의 효과를 평가하고 목표 달성을 위한 후속조치에 대해 매년 대통령, 국가안보보좌관 및 의회에 보고할 방침

• (사례로 얻은 교훈의 통합) 연방정부는 사이버 사고에서 얻은 교훈의 우선순위를 설정하고 해당 전략 구현에 적용할 예정

- 사이버안전심의위원회(CSRB)는 Log4j 취약점에 대한 첫 번째 검토를 완료, 그 동안 취약점 발견부터 역사상 최대 규모의 사이버 사고 대응 진행에 이르기까지 발생한 일에 대한 권위 있는 자료를 생성

- CSRB가 검토를 마치면 연방 정부는 가능한 경우 행정 조치를 통해 자체 운영을 개선하여 권장 사항을 처리하고 필요에 따라 권한을 강화하기 위해 의회와 협력할 것

- 연방 기관은 CSRB 권장 사항을 홍보 및 확대하고 사이버 사고로부터 교훈을 배우기 위한 광범위한 국가적 노력 필요하며 규제 기관은 사고 검토 프로세스를 규제 프레임워크에 구축하도록 권장함

• (투자실행) 전략에 포함된 많은 조치는 보안, 복원력 등 연구 개발에 대한 민간 투자를 늘리기 위한 것이며 연방 기관이 민간 부문을 지원하기 위한 역량을 강화하려면 목표에 대한 투자가 필요

- 국가사이버실(ONCD)는 예산관리실(OMB)과 협력하여 전략에 명시된 목표 달성을 위해 부서 및 기관 예산을 조정하고 연방정부는 사이버안보 활동 자금 지원을 위해 의회와 협력할 방침

[표 27] NCS 전략 6 실행계획 주요 내용

NCS 6 실행계획(NCSIP)	책임기관	완료기한
6.1.1 NCS 실행에 대한 진행 상황 및 유효성 보고 (Report progress and effectiveness on implementing the National Cybersecurity Strategy)	ONCD (국가사이버실)	3분기 FY24
6.1.2 학습한 교훈을 NCS 구현에 적용 (Apply lessons learned to the National Cybersecurity Strategy implementation)	ONCD (국가사이버실)	2분기 FY24
6.1.3 NCS 구현에 따른 예산 지침 조정 (Align budgetary guidance with National Cybersecurity Strategy implementation)	ONCD (국가사이버실)	4분기 FY23

• **이니셔티브 6.1.1 : NCS 실행에 대한 진행 상황 및 유효성 보고**

- ONCD는 NCS의 전략 관련 정책 및 후속 조치의 효과를 평가하고 대통령, 국가안보 담당 차관보, 의회에 첫 번째 연례 보고서를 제공할 것

• **이니셔티브 6.1.2 : 학습한 교훈을 NCS 구현에 적용**

- ONCD는 사이버 사고에서 얻은 핵심 교훈을 파악하고 이를 NCSIP에 적용할 예정이며 연방기관들과 협력하여 사이버 안전 검토 위원회 권장사항을 검토하고 NCS에 반영 여부를 결정할 예정

• **이니셔티브 6.1.3 : NCS 전략 구현에 따른 예산 지침 조정**

- ONCD는 OMB와 협력하여 중앙부처에 대한 사이버보안 예산 우선순위에 대해 공동으로 발행한 연간 지침이 국가 NCS와 일치하도록 조정하고 사이버 생태계 변화 속도에 발맞추기 위해 사이버보안 활동에 자금을 투입할 계획

Ⅱ

’23년 미국 Cybersecurity 정책 추진 현황

2-1 미국 National Cybersecurity Strategy(NCS) 관련 정책

▮ U.S. Cyber Trust Mark Program 발표(백악관, ’23.7.18)

- 백악관은 미국 소비자들이 보다 더 안전하고, 사이버 공격에 덜 취약한 스마트 기기를 더 쉽게 선택할 수 있도록 돕는 사이버 보안 라벨링 프로그램(U.S Cyber Trust Mark Program)을 발표(NCS 실행계획 3.2.2)
- CISA를 포함한 행정부는 FCC(연방통신위원회)와 협조하여 소비자들이 구매 결정을 내릴 때 라벨을 확인하도록 알리고, 소매업체들이 라벨이 부착된 제품을 배치할 때 우선적으로 고려하도록 권장
- FCC는 소비자 인식제고 교육 및 소매업체가 라벨 부착 제품을 우선 배치하도록 장려하고 보안 인증제품이 국가 레지스트리에서 조회될 수 있도록 연결되는 QR코드 운영 등 프로그램 신뢰 유지를 위함 감독 및 집행계획 수립
- NIST는 컨슈머급 라우터에 대한 사이버 보안 요구사항을 정의하기 위한 작업을 즉시 추진하고, FCC가 프로그램에 소비자 등급 라우터를 포함할 수 있도록 하기 위해 해당 요구사항을 2023년 말까지 완료할 계획
- 미국 에너지부 또한, National Labs 및 업계 파트너와 함께 스마트 미터 및 전력 인버터에 대한 사이버 보안 라벨링의 요구사항을 연구하기 위한 공동 계획을 발표
- 미국 국무부는 동맹국과 파트너의 참여를 통해 국제적으로 FCC의 프로그램을 표준화하거나 유사한 라벨링 프로그램에 대한 상호 인증을 지원할 계획
- 이 프로그램은 NIST에서 발표한 사이버 보안 기준[19]에 따라 수립된 프로그램의 개요를 설명하고 2024년 말까지 프로그램 출시에 대한 공개 의견을 구한 후 시행될 예정

▮ 사이버보안 규제 조화 계획 수립을 위한 RFI[20] 발표(국가사이버실, ’23.7.19.)

- 국가사이버실(ONCD)은 사이버보안 규제 조화 계획 수립을 위한 RFI를 발표하여 ’23년 10월 31일까지 이해관계자들의 의견 수렴을 진행함(NCS 실행계획 1.1.1)

– 규제가 중복되는 기존 과제를 파악하고 규제 기관들이 기준 요건을 준수함에 있어 상호주의를 위한 프레임워크를 탐구하기 위함이라 밝힘

19 △ 고유하고 강력한 기본 암호, △ 데이터 보호 방안, △ 소프트웨어 업데이트 및 사고 감지 기능 등
20 Requset for Information : 정보요청

▮ 국가 사이버보안 인력 육성 및 교육 전략 발표(국가사이버실, '23.7.31.)

- 바이든 행정부는 '23년 7월 31일 국가 사이버 노동력 및 교육 전략(NCWES, National Cyber Workforce and Education Strategy)을 발표함(NCS 실행계획 4.6.1)

– 국가 사이버 인력에 대한 다양성 및 사이버 교육훈련에 대한 접근성 확대와 미국인들이 사이버 분야로의 진로 선택을 장려하고 지원하기 위해 해당 전략을 수립

- 연방정부는 파트너와의 협력을 통해 사이버 교육 및 인력 개발을 위한 지역 생태계 활성화와 사이버 기술의 평생교육 지원, 인력 양성의 다양성 향상을 통해 사이버 인력 성장을 지원하고 있음

– (기본적인 사이버 기술 학습 기회 제공) 모든 미국인이 기본적인 사이버 기술을 습득하게 하고 사이버 기술과 관련 분야 경력 추구를 강화할 예정

– (사이버 교육 혁신) 숙련된 사이버 인력에 대한 수요를 즉각적으로 해결하고 학습자가 자발적으로 기술 환경의 미래 요구 사항을 충족하도록 지원하고 사이버 교육을 개선하기 위한 생태계를 구축할 계획

– (국가 사이버 인력 확대) 다양한 이해관계자와 협력하고 인력 채용 및 개발 부분에 있어 기술 기반의 접근 방식을 채택하여 모든 미국인의 사이버 직무에 대한 접근성 증대

– (연방 사이버 인력 강화) 연방정부의 협업 강화를 바탕으로 지속적인 발전을 도모하면서 자격을 갖춘 사이버 인력을 유치하여 인력들의 경력 경로를 개선하고 인사 역량 및 인력에 투자할 방침

- 사이버 인력 양성 및 교육을 위해 연방정부의 주요 기관 및 단체 등과의 파트너십을 통해 NCWES의 목표와 비전을 성공적으로 달성할 것

– (국립과학재단, NSF) NSF는 CyberCorps®에 2,400만 달러 이상을 투자하여 연방, 지방, 주 등 정부에서 근무하는 경력을 쌓을 수 있도록 지원하여 사이버 보안 전문가를 모집하고 유지하는데 지원할 것

– (국가안보국, NSA) NCAE-C[21] 프로그램을 통해 공인된 미국 대학에서 4개의 새로운 사이버 클리닉을 개발하기 위한 시범 이니셔티브를 지원하기 위한 보조금을 발표할 예정

– 사이버 클리닉은 지역 사회와 소규모 정부를 지원하고 200명 이상의 학생들에게 역량 개발의 기회를 제공하고 '24년 말까지 NCAE-C 지전 기관을 460개로 늘려 연간 174,000명의 학생을 지원할 계획

– (국가사이버실, ONCD) 유색인종, 장애인 등 사회적 비주류에 대한 채용과 지원을 늘려 해당 인력이 지역사회에 도달하는 데 초점을 두고 '24년 여름까지 기간을 두어 채용할 예정

– (국립표준연구소, NIST) RAMPS[22] 사이버 보안 교육 및 인력 개발 프로젝트에 최대 3백 60만 달러 지원

– (사이버 보안 및 인프라 보안국, CISA) 매년 10월 사이버 보안의 달을 통해 사이버 인력의 다양성을 장려하고 연방 사이버 방어 기술 아카데미(CDA) 운영을 통해 사이버 방어 분석가 양성을 지원

– 그 밖에도 노동부, 인사관리실, 재향군인회, 주택도시개발부, 구글, MS 등이 사이버 인력 양성 및 교육 강화를 위해 지원을 확대 방안을 발표

21 National Center of Academic Excellence in Cybersecurity
22 Regional Alliance and Multistakeholder Partnerships to Spimate

▮ 오픈소스 소프트웨어 보안 RFI 발표(국가사이버실, '23.8.10.)

• 국가사이버실(ONCD)은 예산관리실(OMB), 연방 최고정보책임자 사무소(OFCIO)와 함께 오픈소스 소프트웨어 보안 이니셔티브(OS3I) 설립(NCS 실행계획 4.1.2)

– 오픈소스 소프트웨어 이니셔티브(OS3I)는 CISA, NSF, DARPA[23], NIST 등과 협력하여 오픈소스 소프트웨어 보안 우선순위를 설정하고 정책 솔루션을 개발하고 있음

• 이에 따라 국가사이버실(ONCD)은 '23년 8월 10일부터 동년 10월 9일 까지 오픈소스 소프트웨어 보안에 대한 이해관계자들의 의견 수렴을 진행함

▮ 에너지부문 보안 설계를 위한 사이버보안 리소스 공개(에너지부, '23.9.6.)

• '23년 9월 6일 에너지부는 에너지보안 및 비상 대응 사무국(CESER)을 통해 국가 사이버 정보 엔지니어링(CIE) 전략 구현을 지원하기 위한 가이드와 리소스를 CIE 실무자 워크숍을 통해 공개(NCS 실행계획 4.4.1)

– (CIE 리소스 라이브러리) CIE 리소스 라이브러리는 CIE 원칙을 적용할 때 설계자, 제조업체, 자산 소유자 및 운영자를 지속적으로 지원하는 도구, 사례 연구 및 강의로 구성

– (CIE 구현 가이드) CIE 구현 가이드는 엔지니어링 팀이 CIE 원칙을 적용하기 위해 시스템 수명 주기의 각 단계에서 고려해야 요소들을 설명

▮ 국방부 사이버전략(국방부, '23.9.12.)

• 국방부 사이버전략은 중국 · 러시아 · 북한 · 이란의 사이버 위협과 초국적 범죄 조직들의 사이버 위협 대응을 위한 국가사이버안보전략(NCS)의 실현 방안을 다룸(NCS 실행계획 2.1.1)

• 미 국방부는 사이버 위협 대응을 위해 △국가 방어 △ 전투 준비와 전쟁에서 승리 △ 동맹 및 파트너 국가와 연대 △ 사이버 공간에서 미국의 지속적인 이익 추구라는 네 가지 핵심 전략을 다음과 같이 공개

– (국가 수호) 국방부는 사이버 공간에서의 캠페인을 통해 악의적 행위자의 역량과 지원 생태계를 파괴할 것이며 기관 간 파트너십을 통해 중요 인프라를 방어하고 군사 준비 태세에 대한 대응역량을 강화할 예정

– (승리 준비) 국방부 정보 네트워크의 사이버 보안을 위해 방어적인 사이버 공간 작전을 수행하고 합동군의 사이버 회복력과 사이버전 역량 강화 및 비대칭 우위를 달성할 계획

– (동맹국 및 파트너와 사이버 도메인 보호) 동맹국 및 파트너의 역량 강화를 지원하고 지속적인 기술 협력 및 사이버 공간에서의 규범 준수를 장려하여 악의적 행위자의 위협 방지와 책임 있는 국가 행동을 강화

– (사이버 공간에서 이점 추구) 제도 개선을 통해 군이 보유한 사이버 관련 조직 · 훈련 · 장비 등을 강화하고 사이버 작전 지원을 위한 정보의 가용성 보장과 국방 기업 전반에 걸쳐 사이버 보안 인식 문화를 조성

23 국방고등연구계획국

▮ 사이버안전검토위원회(CSRB) 필수 조직화(국토부, '23.9.21.)

• '23년 4월 24일 미 국토부 장관은 CSRB[24]를 공식 조직으로 설립하도록 촉구하는 성명 발표와 함께 해당 조직을 필수 조직화 하기 위한 법안 초안을 공개(NCS 실행계획 1.4.4)

• 국토부는 '23년 4월 24일 투표를 통해 입법안을 승인하고 의회에 제출하였으며 '23년 9월 21일 의회 승인에 따라 헌장[25]됨

- CSRB는 연방민간행정기관(FCEB)의 정보 시스템 또는 비연방 시스템에 영향을 미치는 중대한 사이버 사고와 관련하여 위협 활동, 취약성 완화 활동 및 기관 대응을 검토 및 평가

▮ 오픈소스 사이버보안 가이드라인 발표(CISA, FBI, NSA, DOT, '23.10.10.)

• CISA는 FBI, NSA 및 미 재무부(DOT)와 협력하여 운영기술(OT) 및 산업 제어 시스템(ICS) 환경에서 오픈소스 소프트웨어의 안전한 사용을 위한 모범사례 및 권장 사항 등을 공개(NCS 실행계획 4.1.2)

- (권장사항 ①) 오픈소스 소프트웨어 생태계를 지원하고 소프트웨어 개발 과정 전반에 걸친 보안 툴 및 모범 사례 등이 적용될 수 있도록 지원

- (권장사항 ②) 오픈소스 소프트웨어와 운영기술(OT) 고유의 특성 때문에 기관과 기업들은 취약점 관리를 단순화하기 위해 같은 취약점 식별 방법을 사용할 것을 권장

- (권장사항 ③) OT 시스템을 재부팅하여 패치를 적용할 때 비용 절감을 위해 별도의 패치 배포 방법이 필요하며 ICS의 경우 소프트웨어 개발 프로세스를 간소화하는 업데이트가 필요함

- (권장사항 ④) 인증 및 권한 부여 정책을 개선하여 고유하고 검증 가능한 사용자 계정을 사용하고 하드코딩 된 자격 증명, 취약한 구성을 파악하여 중앙 집중식 사용자 관리 솔루션을 구현해야함

- (권장사항 ⑤) 오픈소스 프로그램 오피스 개발 및 지원을 통해 오픈소스 소비 관행 개선, 소프트웨어 자산 인벤토리 유지 관리를 위함 공통 프레임워크 설정이 요구됨

▮ 랜섬웨어 근절 가이드 발표(JRTF, '23.10.19.)

• CISA와 FBI가 공동의장을 맡은 JRTF[26]는 랜섬웨어 공격에 대한 정부 기관과 민간 부문 파트너 간의 정보 공유 및 협력을 촉진하고 랜섬웨어에 대응하기 위한 업데이트된 가이드 발표(NCS 실행계획 2.5.2)

- 랜섬웨어 공격 예방 및 대응과 관련된 모범 사례 개발 및 공유, 랜섬웨어 위협 행위자에 대한 공동 조사 및 작전 수행, 랜섬웨어 피해 기관 · 기업에 복구 지침 및 리소스 제공 등의 활동을 수행할 예정

24 행정명령 14028에 따라 설립되어 사이버사고 검토 및 평가와 민간·공공 부문에서 개선이 필요한 안건을 제시하는 심의 기능을 수행
25 헌장 : 국가, 기관 등에서 정립한 규범이나 법과 같이 구속력, 강제성, 처벌성 등을 지니지 않음

▮ Secure by Design 가이드라인 개정(CISA, '23.10.25.)

• CISA는 NSA, FBI와 협력해 17개의 국제 파트너의 의견을 반영한 "설계 기반 보안 소프트웨어를 위한 원칙 및 접근 방식"에 대한 새로운 지침을 발표함(NCS 실행계획 1.2.1)

• 해당 지침은 소프트웨어 제조업체를 위한 권장 사항으로 사용될 예정이며 소프트웨어 시스템 및 모델 제조업체가 제품 생산 시 준수해야 할 세 가지 핵심 원칙을 공개

- (원칙 ①) 보안에 대한 부담과 책임을 고객과 제조업체가 함께 가져야 하고 보안을 기본으로 하는 관행, 안전한 제품을 개발하는 관행, 보안을 최우선으로 하는 비즈니스 관행들을 형성할 것
- (원칙 ②) 제조업체는 안전한 제품을 제공함에 있어 타 제조업체와 차별화되는 투명성이 있어야 하며 이를 위해 강력한 인증 메커니즘 활용과 공통 취약성 및 노출 기록이 정확할 수 있도록 전략을 수립해야 함
- (원칙 ③) 기술 분야의 전문 지식은 제품 보안에 핵심적인 요소이지만 해당 기술들이 제품에 모두 반영되기 위해서는 경영진의 의사결정이 필수적이기에 보안 문제를 충분히 고려한 회사 차원의 리더십을 개발해야 함

2-2 한국 Cybersecurity 관련 정책

▮ K-사이버방역 추진전략(과학기술정보통신부, '21.2.18.)

• 과학기술정보통신부는 제13차 정보통신전략위원회에서 정보보호 패러다임 변화에 대응하고 안전하고 신뢰할 수 있는 디지털안심 국가 실현을 위한 "K-사이버방역 추진전략"을 발표

- '23년 까지 총 6,700억 원을 투자하여 ① 디지털안심 국가 기반 구축, ② 보안 패러다임 변화 대응 강화, ③ 정보보호산업 육성 기반 확충 등 3대 중점 전략과 8개의 과제를 공개

[표 28] K-사이버방역 추진전략 추진 전략 및 과제

3대 중점 전략	전략 과제
1. 디지털안심 국가 기반 구축	1-1. 사이버보안 대응체계 고도화 1-2. 수요자 중심 디지털보안 역량강화
2. 보안 패러다임 변화 대응 강화	2-1. 차세대 융합보안 기반 확충 2-2. 신종 보안위협 및 AI 기반 대응 강화 2-3. 디지털보안 핵심기술 역량 확보
3. 정보보호산업 육성 기반 확충	3-1. 정보보호산업 성장 지원 강화 3-2. 디지털보안 혁신인재 양성 3-3. 디지털보안 법제도 정비

출처) 과학기술정보통신부, "K-사이버방역 추진전략" 재정리

▮ 랜섬웨어 대응 강화방안(과학기술정보통신부, ’21.8.5.)

• 미국 콜로니얼 파이프라인 랜섬웨어 사건을 비롯해 국내 · 외 랜섬웨어 피해가 증가함에 따라 랜섬웨어 맞춤형 대응 지원체계 구축 및 선제적 예방과 핵심 대응역량 강화를 위한 전략 마련

– △ 국가중요시설 – 기업 – 국민 수요자별 선제적 예방, △ 정보공유 – 피해지원 – 수사 사고 대응 全주기 지원, △ 진화하는 랜섬웨어에 대한 핵심 대응 역량 제고

▮ 정보보호산업의 전략적 육성 방안(과학기술정보통신부, ’22.2.10.)

• 국가 차원에서 정보보호산업을 전략적으로 육성하여 사이버보안 대응력을 강화하여 디지털 자산을 보고하고 새로운 경제 성장 기회로 활용하기 위해 4가지 전략을 소개

– (① 성장 동력 확보를 위한 정보보호 新시장 창출) 인공지능 보안, 비대면 보안, 등 정보보호 新시장 창출을 통한 성장 동력 확보

– (② 글로벌 일류 정보보호기업 육성) 선도기술 및 제품 개발과 M&A 활성화 및 해외진출 확대를 통한 글로벌 일류 보안기업 육성

– (③ 정보보호산업 기반 강화를 위한 생태계 확충) 정보보호공시제도 의무화, 정보보호 인증 고도화, 중소기업 및 지역 사이버보안 역량 강화 등 지속성장을 위한 산업 생태계 조성

– (④ 차세대 정보보호 기술경쟁력 확보) 정보보호산업 성장을 뒷받침하고, 안전한 디지털 전환을 위한 정보보호 핵심 원천기술 확보

▮ 사이버 10만 인재 양성 방안(과학기술정보통신부, ’22.7.13.)

• 사이버보안 산업 수요에 대응하는 인력의 양적 확대와 최정예 화이트해커, 보안개발자 양성 등 인력의 질적 강화를 함께 도모하고 누구나 교육을 받고 성장할 수 있도록 교육 저변 확장을 위한 전략 발표

• 실전형 사이버 인력 10만명 양성, 최정예 전문 인재 2,000명 육성, 우수 보안 스타트업 25개 창업 지원을 통해 민간의 우수 인적자원을 활용한 국방 · 치안 분야 사이버 역량 제고를 위해 3가지 전략을 수립

– (① 사이버보안 개발부터 대응까지 全주기 최정예 인력 양성체계 구축) 융합보안대학원(’22년 8개 → ’26년 12개)과 정보보호특성화대학(’22년 3개 → ’26년 10개)을 확대 및 개편

– “시큐리티 아카데미”(’23~, 200명)를 도입하여 기업 내 사이버보안 의사결정자(CEO, CISO 등) 인식제고 및 중소기업 보안인력 교육지원 강화

– IT개발 인력을 선발하여 보안교육 · 창업을 지원하는 “S-개발자” 과정 신설(’23~, 50명), 화이트해커에 잠재력 있는 보안 인재 육성을 위해 “화이트해커 스쿨” 과정(’23~, 300명) 신설

– (② 저변 확대를 위해 상시 육성 체계와 글로벌 연계 기반 마련) 실전형 “사이버훈련장”을 확대하고 실제사고에 대응 가능한 훈련 시나리오와 멀티 훈련 플랫폼 개발

– 지역 보안인재 육성을 위해 지역교육센터를 중심으로 거점대학과 함께 교육을 지원하고 “지역 정보보호 협의회”를 구성하여 지역 인재 양성과 지역 사이버 산업 육성의 선순환 구조 마련

- (③ 민 · 관 · 군 유기적 협력으로 사이버 전 · 범죄 대응) 사이버작전 및 수사 분야 전문대 · 대학 · 대학원 과정신설과 軍 사이버 인력의 운영 개선을 통해 군 경력 우수 인재의 민간 유출 방지
- 軍 사이버안보 분야 근무자 취업 연계 지원하는 "사이버 탈피오트" 도입 및 공공기관 정보보안담당자의 역량 강화를 위해 지역대학과 연계한 지방거점 사이버안보 교육체계 구축

▮ 정보보호산업의 글로벌 경쟁력 확보 전략(과학기술정보통신부, '23.9.5.)

• 과학기술정보통신부는 글로벌 정보보호산업 경쟁력 강화를 위해 '27년까지 정보보호산업 시장규모 30조원 달성, 보안 유니콘 기업 육성 등을 목표로 4가지 전략과 세부과제 발표

- (① 보안패러다임 전환 주도권 확보 및 新시장 창출) 새로운 보안체계 적용과 미래 산업의 보안내재화를 통해 新시장을 창출하고, 융합보안 및 물리보안 산업 강화를 통해 글로벌 보안시장 진출 확대
- (② 협업 기반 조성을 통한 신흥시장 진출 강화) 기업 간 협력을 기반으로 한국형 통합보안 모델을 구현하고, 신흥시장을 전략적으로 공략하여 글로벌 시장 경쟁력 확보
- (③ 글로벌 공략을 위한 단단한 산업 생태계 확충) 우리 보안기업의 글로벌 시장진출 가속화를 위해 시설확충 · 펀드조성 · 인재양성 등 지속성장 환경 조성에 집중 투자
- (④ 차세대 정보보호 기술 경쟁력 확보) 미래 산업 성장에 필수적인 전략기술 개발에 집중하고, 선도국과의 공동연구 추진으로 글로벌 기술 패권 경쟁에서 우위를 점할 수 있는 기술력 확보

▮ 한국은 앞서 소개한 Cybersecurity 정책들과 더불어 "국가 사이버안보 역량강화"를 세부 과제로 담은 국가 안보전략을 발표한 바 있음

• 총 6가지의 전략과제를 담고 있으며 그 중 6번째 전략과제인 "신안보 이슈에 능동 대응" 전략의 세부과제로 "국가 사이버안보 역량 강화"를 공개함('23.6.7.)

- (① 국가 차원의 일원화된 대응체계 구축) 사이버안보 위협에 대응하기 위해 국가안보실을 중심으로 각급기관의 역할 및 협력체계를 확립하고, 이를 반영한 "사이버안보법 " 제정
- (② 글로벌 사이버안보 위협에 대한 대응 활동 강화) 악의적인 사이버공격에 총동원하여 공세적으로 대응하며 국가를 배후로 둔 해킹조직들의 활동을 중점 감시
- (③ 국제사회와 사이버안보 공조 강화) "사이버범죄협약" 가입 추진 및 '23년 4월 "전략적 사이버안보 협력 프레임워크" 채택을 통해 한미동맹을 강화하고 사이버 공간에서의 위협을 효과적으로 대응
- (④ 사이버안보 기반 역량 강화) 사이버사고 발생 시 정상 상태로 복원하기 위한 사이버보안 대책과 피해복구 방안을 구체화하고 사이안보에 필요한 기술 · 정책개발과 인재 양성을 강화할 예정

Ⅳ 시사점

▮ 미국은 Cybersecurity에 대한 글로벌 인식의 변화에 발 빠르게 후속 계획을 마련

- 첫 번째 전략인 주요 인프라 방어 전략은 주요 기반시설 및 핵심 서비스에 대한 사이버 복원력 확보 및 민 · 관의 협력을 강조하고 있음

– 미국의 인프라 방어 전략은 한국의 주요 기반시설 보호체계와 같은 방향성을 가지고 있으나 세부 과제들을 검토하여 한국 기반시설보호 체계의 미비점을 파악하여 보완에 대해 논의할 필요성이 있음

- 두 번째로 미국은 사이버 공간을 위협하는 행위자들에 대한 예방 및 대응역량 향상뿐만 아니라 사이버 공격의 결과로서 얻은 이익의 무력화 방안과 사이버 범죄자의 책임 강화를 위한 협력 과제 등을 소개

– 한국 역시 랜섬웨어를 포함한 사이버 공격으로 인한 수익을 국내 세탁 및 활용이 불가능하게 하는 조치가 필요하며 이를 위해 부문 간의 협력 대상을 기존보다 확대되어야 함

- 세 번째, 연방정부는 공급망 안전성 확보를 목표로 사이버보안 산업이 안전한 제품을 개발 할 수 있는 환경을 조성

– 미국의 공급망 안전성 강화 정책으로 인해 한국의 소프트웨어 및 소프트웨어 포함 제품 수출시 피해가 발생하지 않도록 이와 관련된 공공 분야 및 민간분야 간의 협력과 공조가 요구됨

- 네 번째, 미 정부는 차세대 디지털 인프라 구축을 통해 인공지능 및 양자컴퓨팅 등의 혁신적인 변화를 적극적으로 수용하고 이를 활용하여 사이버 복원력을 확보 · 강화하고자 함

– 차세대 ICT 신기술로 인한 위협 요인 및 대비책 등을 선도적으로 마련해야하며 인공지능, 양자 컴퓨팅 등 신기술을 통한 보안 생태계 변화 등을 전망하여 기관, 기업, 개인이 새로운 유형의 사이버 위협을 대비할 수 있는 전략 및 지원책 마련이 요구됨

- 마지막으로 NCS 전략 목표를 효과적으로 달성하고 세부 과제 수행을 통한 국가 사이버 역량 강화를 위해 공공 · 민간분야 협력과 우방국 및 파트너와의 국제적인 협력이 필수적임을 언급하고 있음

– 한국은 미국, 영국, 네덜란드와 사이버 동맹을 통해 관련 분야 협력체계 구축했으며 이와 같이 지속적으로 군사 · 경제적 동맹 관계를 사이버 공간까지 확장하는 노력을 지속해야 함

▮ 디지털 전환 가속화로 사이버 위협이 산업 · 사회 · 안보 全 영역으로 확대 · 지능화되고 있기 때문에 민간 · 공공 협력을 바탕으로 하는 포괄적 대응 필요

- 선제적 대응이 가능한 사이버 방어 정책 전환이 요구되며 이를 위해 사이버 공격으로 피해가 발생되기 이전에 공격자의 의도를 미리 분석하여 사전 조치가 이루어져야 함
- 민관협력 체계 구축을 바탕으로 사이버 위기 대응을 위한 新기술 R&D 투자와 민간기업의 Cybersecurity 역량 강화를 도모하여 사이버 위협 공동 대응 체계 구축이 필요
- 국제 협력 체계의 적극적인 참여를 통해 사이버위협정보공유, 사이버 합동훈련 실시 등 국제공조를 통한 국가사이버 방어역량 강화와 사이버 복원력을 확보 필요

KISA

INSIGHT

DIGITAL & SECURITY POLICY

2024 VOL. 01

KISA 한국인터넷진흥원