

미국 AI 행정명령(E.O. 14110)의 이행 현황¹⁾

서울대 법학전문대학원 교수 박상철

2024. 12. 15. 간행 예정인 논문에 활용될 것이므로, 그 전까지 인용 및 전재를 금합니다.

1. E.O. 14110의 이행 현황

미 바이든 행정부의 2023. 10. 30.자 “인공지능의 안전·안보·신뢰성 있는 개발·이용에 관한 행정명령”(E.O. 14110)은 연방기관들에 관할 분야별로 과업을 부여했고, 지난 1년간 과업들이 대부분 이행되었다. 그 중 공개된 규정·가이드라인·보고서를 중심으로 열거·요약하면 이하와 같다.

[표 1: E.O. 14110의 이행 현황]¹⁾

항목	기관 [부서]	문서명	내용	일자	E.O. 14110
제4장 (안전과 안보/보안)					
생성AI와 이중용도 기반모델 등의 평가관리	국가표준기술원 (NIST)	AI 리스크 평가 프레임워크(AI RMF): 생성AI 프로파일(NIST AI 600-1)	생성AI에 대해 리스크 지목 및 AI RMF 1.0상 리스크 평가 항목 추가	24/7/25	4.1(a)(i)(A)
		합성콘텐츠로 인한 리스크 경감(NIST AI 100-4)	합성콘텐츠 투명성 확보(출처데이터추적, 합성콘텐츠탐지) 및 아동성착취물, 비동의사적이미지 피해 예방 메커니즘	24/4 (초안)	4.5
		생성AI와 이중용도 기반모델을 위한 보안성 있는 소프트웨어 개발 프레임워크(SSDF): SSDF 커뮤니티 프로파일(NIST SP 800-218A)	사이버보안 행정명령(E.O. 14028)에 따른 SSDF 1.1에 생성AI 및 이중용도 기반모델 관련 사항(AI모델 특유의 취약성과 위협 유형 및 모델가중치와 설정파라미터 보안 등) 추가	24/7/26	4.1(a)(i)(B)
	NIST [AIS]	이중용도 기반모델 오용 리스크 관리(NIST AI 800-1)	이중용도 기반모델의 오용 유형 식별 및 오용 리스크 관리 목표 설정	24/7 (초안)	4.1(a)(ii)
보고의무	상무부 (DOC) [BIS]	향상된 AI모델과 컴퓨팅 클러스터에 대한 보고요건의 설정(15 CFR Part 702) 개정안	국방물자생산법(DPA)에 근거한 이중용도 기반모델(연산량 1026 OP 이상)과 대규모 컴퓨팅 클러스터(300Gbit/s, 1020 OP/s 초과)의 분기별 보고의무	24/9/11 (입법예고)	4.2(a), (b)
	상무부 (DOC) [BIS]	중대한 악성 사이버 공격 관련 국가비상사태 대응을 위한 추가 조치(15 CFR Part 7) 개정안	국제긴급경제권한법(IEEPA)와 국가비상사태법(NEA)에 근거한 클라우드 인프라 서비스(IaaS) 제공자의 외국인 거래 및 대규모 모델 훈련 보고의무	24/1/29 (입법예고)	4.2(c), (d), (e)

1) 필자와 관련 논문을 집필 중인 김장 법률사무소 양수빈, 이대준 변호사와 서울고등법원 신원준 재판연구원이 표를 함께 작성하였다.

보안	국토안보부 (DHS) [CISA]	주요기반시설 보유운영자를 위한 안전·보안 가이드라인	16개 주요기반시설의 AI 용례 식별, 유형화, 리스크 지목, NIST RMF 1.0의 체계에 맞춰 프로세스 구체화	24/4/26	4.3(a)(iii), (iv)
	CBRN	금융서비스 부문에서의 AI 특유의 사이버보안 리스크의 관리	AI로 인한 금융에 대한 새로운 보안 위협 대응을 위한 모범사례	24/3	4.3(a)(ii)
CBRN	DHS	AI와 CBRN 위협의 접점에서의 리스크의 경감에 관한 보고서	AI의 CBRN 오용 관련 핵심 쟁점을 정리하고, 대책을 제시	24/4/26	4.4(a)(i)
	국가과학기술 위원회(NSTC)	핵산 합성 스크리닝 프레임워크	AI 기반 합성핵산염기서열 제공자의 구매 스크리닝 절차 규정	24/4 제정, 24/9 개정	4.4(b)
공개모델	DOC [NTIA]	널리 가용한 모델 가중치를 가진 이중용도 기반모델	오픈소스 대규모 범용모델의 편익과 리스크, 제한 필요성 검토	24/7/30	4.6

제5장 (혁신과 경쟁)

해외 AI 인재의 미국 유치	DHS [USCIS]	비이민 범주(8 CFR Part 214) 개정	비이민 취업비자인 H-1B 등록 절차 간소화	24/2/2	5.1(a)
	노동부(DOL)	미국 내 외국인의 정규직 노동허가절차(20 CFR Part 656) 개정안	정규직 취업허가 절차 현대화	24/2/15 (입법예고)	5.1(e)
연구개발 진흥	DOE	에너지를 위한 AI: 그리드 현대화 및 청정에너지 경제를 위한 기회	청정에너지 목표 달성을 위해 AI 용례 탐색, 전력망 적용 AI 모델의 보안 및 편향 리스크 해결 및 견고성 촉진	24/4	5.2(g)
	대통령실 과학기술자문 위원회(PCAST)	연구 진흥: AI를 활용한 글로벌 문제 해결	AI를 통해 글로벌 문제를 효과적으로 해결할 방법과 AI 활용으로 인한 리스크를 해결하기 위한 윤리적인 사용과 자원의 공정한 접근을 보장	24/4	5.2(h)
지식재산권	특허상표청 (USPTO)	AI 지원 발명에 대한 발명자 적격 지침	AI 지원 발명은 AI가 발명자 적격이 없음을 명확히 하고 특정 자연인의 발명 기여 판단기준 제시	24/2/13	5.2(c)(i)
		특허심사기준(MPEP) § 2103- 2106.07(c) 개정	AI 지원 발명의 특허 적격성 판단 기준과 사례 제시	24/7/17	5.2(c)(ii)
	DHS	2024 AI 로드맵	AI 관련 지식재산권 보호를 위한 정책 로드맵 제시	24/3/17	5.2(d)(i), (ii)

제6장 (노동자 지원)

노동시장 영향 연구	대통령실 과학기술자문 위원회(PCAST)	AI의 잠재적 노동시장 영향: 실증 분석	AI의 노동시장 영향을 장기적 관점에서 분석할 필요가 있으며 단순한 AI 노출도가 아닌 각 직무에서의 AI 용례 등 다양한 기준을 고려해야 한다고 결론	24/7	6(a)(i)
노동자 피해 최소화	DOL	인공지능과 노동자 안온(well- being)	직장 내 AI 활용과 관련하여 원리와 모범규준을 제시	24/10/19	6(a)(i), (b)(i), (ii)
근로기준		공정노동기준법(FLSA) 및 기타 연방 노동기준의 적용 관련 직장 내 AI 및 자동화 시스템 이용 지침을 위한 현장지원안내서	직장 내 AI 및 자동화 시스템 활용 시 FLSA 상 문제를 지적하고 인적 감독의 필요 강조	24/4/9	6(b)

제7장 (AI 편향과 시민권)					
형사사법 차별	법무부(DOJ)	-	민권 담당 법무차관보가 유관기관들과 사법 집행 과정에서 AI가 야기할 수 있는 차별 등 시민권 침해 등의 해결 방안에 대해 수차례 협의 중	-	7.1(a)
		-	형사사법체계에서 AI 사용에 관한 검토 중. 산하 사법연구소(NIJ)가 의견제출요청	-	7.1(b)
		법무부의 공무원 구인·임용·승진·보유를 위한 모범실무 관련 주·부족·지방·준주 사법집행기관 지침	AI 관련 기술 전문성을 갖춘 법집행 전문가들의 임용 방안 제시	23/11	7.1(c)(i), (ii)
공공부조 차별	보건복지부 (HHS)	공공부조 행정에 있어 주·부족·지방·준주정부의 자동화 알고리즘 시스템에서 AI의 책임 있는 사용을 촉진하기 위한 계획	공공부조 분야에서 권리 또는 안전에 영향을 미치는 AI 용례 파악, 활용 촉진 정책 제시	24/4/29	7.2(b)(i)
	농무부(USDA)	공공부조 행정을 위한 주·부족·지방·준주의 AI 사용에 대한 프레임워크	현물(식품) 공공부조 관련. 내용은 위와 같음.	24/4/29	7.2(b)(ii)
주거 차별	주택도시개발부 (HUD)	AI 적용에 관한 공정주택법 가이드라인	AI 기반 임차인 심사 및 디지털 플랫폼을 통한 부동산 거래 광고에 대한 공정주택법 적용 논의	24/4/29	7.3(b), (c)
제8장 (소비자 보호)					
보건복지	HHS	-	범부처 태스크포스가 보건복지 AI 보고서 작성 중	-	8(b)(i)
	HHS [OCR]	의료비용합리화법(ACA) § 1557에 대한 행정규칙(45 CFR Part 92) 개정안	보건 프로그램 관련 AI 활용이나 자동화 여부를 불문하고 차별이 금지되어야 함은 명기	24/5/6 (입법예고)	8(b)(iii)
교통	교통부(DOT) [NETT Council]	-	교통부 산하 기관별 AI 용례와 잠재적 영향 분석 중	-	8(c)(i)
교육	교육부(MOE) [OET]	AI를 활용한 교육의 설계: 개발자들을 위한 필수 지침	교육 분야 AI 제품 개발자들의 신뢰 확보를 위한 지침	24/7	8(d)
제9장 (프라이버시)					
프라이버시	대통령실 관리에산실 (OMB)	-	프라이버시 보호 영향 평가 작업 중: 기관들이 수집하는 상업적 이용 가능 정보(CAI)의 보유·보고 절차 평가 표준 등	-	9(a)
	NIST	차분프라이버시(DP) 보장 평가 지침서	DP 보장 평가에 대한 지침 제시	23/12/11 (초안)	9(b)
제10장 (연방의 AI 활용 촉진)					
AI 활용 촉진	OMB	기관의 AI 활용에 대한 거버넌스, 혁신, 리스크 관리의 진전(M-24- 10)	각 연방기관의 AI 거버넌스의 강화, AI의 책임 있는 혁신의 진전, AI 활용으로부터의 리스크 관리를 규정	24/3/28	10.1(a)-(e)

생성AI 활용	FedRAMP	신흥기술 우선 프레임워크	연방기관 조달 클라우드 제품·서비스의 보안 평가에 있어 생성AI 등 신흥기술 승인의 근거 마련	24/1/26	10.1(f)(ii)
	인사관리처 (OPM)	연방 인력의 책임 있는 생성AI 활용	연방정부 공무원의 공직 수행 과정 생성AI 활용 시 준수사항	—	10.1(f)(iii)
AI 조달	OMB	정부 내 책임 있는 AI 조달 촉진(M-24-18)	AI 시스템 및 서비스의 조달 절차에 M-24-10을 반영	24/9/24	10.1(d)(ii)
	조달청(GSA) [ITVMO]	생성AI 및 특수 컴퓨팅 인프라 확보 리소스 가이드	공공조달 과정에서 생성AI 개발자들에 대한 접근성을 높이는 방안 마련	—	10.1(h)
연방정부 내 AI 인재 확대	OPM	연방정부의 AI 활용의 진전을 위한 범정부 임용 권한	AI 인재 신속 임용을 위해 직접임용권과 특별임용의 근거를 명확히 함	23/12/29	10.2(c), (d)(ii)
		AI, AI 지원 및 기타 핵심기술 인재를 위한 급여, 인센티브, 연차 및 인력 유연성 프로그램	AI 인재 임용 유연성 증진	24/2/27	10.2(d)(i), (iv)
		AI 분류 정책 및 인재 확보 안내서	정부시법에 따라 직무 분류를 명확히 하며 보수·직렬·직책·업무난이도 고려	24/4	10.2(d)(v)
		고위직 핵심 자격	고위직의 AI 관련 항목별 고위급 핵심 자격요건	—	10.2 (d)(vii)
		토목을 위한 AI 역량 모델	토목 AI 활용에 대한 역량 명세	24/4/29	10.2 (d)(viii)
제11장 (국제적 리더십)					
국제표준	NIST	AI 표준에 대한 글로벌 관여 계획(NIST AI 100-5)	AI 표준에 대한 목표와 우선조치를 제시	24/7	11(b)(i), (ii)
국제개발	국제개발처 (USAID), 국무부(DOS)	국제개발에서의 AI 플레이북	AI 관련 국제개발에 있어 권고사항 제시	24/9	11(c)(i)

요약하면 (1) 안전·안보와 관련해서는 이중용도 기반모델(dual-use foundation model)의 화생방핵(CBRN)이나 사이버공격 툴 등으로의 오용, 주요기반시설(critical infrastructure)의 보안, 생성AI의 기만수단이나 아동성착취물(CSAM), 비동의사적이미지(NCII) 등으로의 오용 리스크에 집중하여 대응 체계를 강구하였고, (2) 혁신·경쟁의 촉진을 위해 연구개발 지원 뿐 아니라 해외 AI 인재의 유치, 특허 등 지식재산권의 정비를 추진하였으며, (3) 노동, 시민권, 소비자보호, 프라이버시를 위해 각 기관이 자신의 소관 부문별로 보호를 강구하였고, (4) 연방의 AI 활용과 관련해서는 대통령실 관리예산실(OMB)을 중심으로 각 기관의 AI 활용을 촉진하고 권리·안전영향AI에 대해서는 안전장치를 마련하되, (5) 국제협력을 통해 미국의 리더십을 유지하고자 하였다.

2. 시사점

미국은 안보적으로는 연방 역량을 준전시적으로 결집하며 AI의 공급망 문제에 대해 수출통제에 준하는 접근을 하고 있다. 민간에 대해서는 EU AI법과 같은 수평적·포괄적 접근 하에 중복규제를 양산하기보다는 각 부처가 분야별로 AI의 용례를 파악하고 용례별 리스크에 대한 방대한 연구·검토를 거쳐 기존 규제를 재해석하거나 정비하되 경성규범과 연성규범을 유연하게 조합하며 대응하였다. 또한 연방정부의 AI 활용에 있어 기관 간 활용 경쟁을 촉진하면서도 안전·권리영향AI가 초래할 수 있는 리스크에 대한 대응을 강구하였다. 11월의 미 대선 결과에 따라서는 상당한 정책 변화가 예정되어 있다. 그러나 실질에 있어서는 안전·안보, 혁신·경쟁 중 출입국·이민 이외의 부분, 공공부문과 관련한 기조는 대체로 이어질 것으로 예상할 수 있다. 더욱이 이상의 1년간의 범부처적 검토 내용은 향후 연방의 AI 정책의 주요 참고자료이자 출발점이 될 것이다.

우리로서는 AI에 대해서는 경제와 안보가 더 이상 분리될 수 없는 현실을 직시하고 미국의 안보적 입장에 보조를 맞추어 공급망에 대한 접근의 유지를 기하되, 국내 개발사들의 생존과 유지도 도모하고자 미국의 상기 AI 활용 촉진 정책을 참고하여 공공부문의 AI 조달 수요를 공세적으로 끌어올릴 필요가 있다. 또한, 우리나라는 정치권과 시민사회단체의 EU AI법 계수에 대한 선호와 부처 간 권한 경쟁의 결과 향후 AI 3중규제국(전통 규제법 + AI기본법 + AI이용자보호법)으로 전락할 우려가 큰데, 규제는 미국의 상기 사례처럼 각 부처가 자신이 맡아왔던 기존 분야의 법령을 AI에 맞춰 정비해 나가는 방식으로 일원화(streamline)시켜 준수비용을 최소화할 필요가 있다. AI가 초래하는 사회문제는 동질적이기보다는 맥락별로 이질적이므로, EU식의 수평적·포괄적 규제보다는 부처별·용례별 맞춤형 규제를 해야만 리스크에도 효과적으로 대응하고 인권도 더 두텁게 보호할 수 있다. IT부처들의 AI에 관한 뛰어난 식견과 전문성은, EU식 중복규제에 쓸 것이 아니라, (AI 진흥은 물론이거니와) AI 안전과학 연구, AI의 유형별 연성규범의 제공 등 근본적이며 미래지향적인 사항들에 활용되어야 합당하다. 이러한 IT부처들의 노력이 뒷받침되어야만, 다른 부처들도 기존 규제들을 정연하고 체계적으로 정비할 수 있게 될 것임은 물론이다. 일본이 AI 거버넌스에 대해 지난 1년여간의 숙고를 거쳐 최근 총무성/경제산업성의 AI 전체에 대한 연성규범과 각 부처의 분야별 경성규범을 조합하는 접근법을 선택하였음을 가버이 받아들여선 안 된다. 당장 현안인 AI기본법안은 일단 규제 조항을 분리하여 나머지 조항만 통과시켜야 한다. 이로써 차분한 연구·검토를 위한 시간을 번 후, 범부처적으로 미국이 지난 1년간 검토한 사항을 숙지하고, 우리 특유의 용례와 사회문화적 리스크도 파악하여, 기존 부처별 법령을 정비해 나가야 한다. 🌐