정책이슈리포트 2025-07(02)

미국 매사추세츠주, 「인공지능모델과 안전성을 통한 경제발전촉진법(안)」 발의

대규모 AI모델이 가져올 수 있는 잠재적 위험 관리체계 구축에 대한 시사점

발행일: 2025.07.09.
발행기관: 디지털안전센터
키워드: AI안전사고, 임계적 피해, 사이버 위협, 위험성 평가, 예방적 대응

1. 도입 배경 및 목적

현재 미국은 연방 차원의 포괄적 AI 법률이 부재한 상황에서 각 주가 독자적인 규제 체계를 구축하고 있어 "조각보 같은 규제 환경"을 형성하고 있다. 지난 2024년 한해 동안 47개 주에서 약 600건 이상의 AI 관련 주 법안이 발의(Multistate, 2025)되었으며, 올해에는 이 수치가 더욱 증가될 수 있다.

매사추세츠 주는 인공지능 기술의 급속한 발전과 함께 대규모 AI 모델이 가져올 수 있는 잠재적 위험에 대한 우려 증가에 따라 「인공지능 모델과 안전성을 통한 경제 발전 촉진법(An Act promoting economic development with emerging artificial intelligence models and safety)」을 발의했다. 이 법안은 2025년 1월 17일 Barry R. Finegold 상원의원에 의해 상원 문서 번호 1909번으로 제출되었으며, 2025년 2월 27일 하원 동의를 거쳐 첨단 정보 기술, 인터넷 및 사이버 보안 위원회에 회부되어 현재 심의 중인 상태다.

이 법안은 매사추세츠 주를 AI 혁신의 중심지로 성장시키고, 동시에 무분별한 AI 개발로 인한 사회적 위험을 최소화하고자 기술 중심 주들 간의 일관된 AI 보호 조치를 마련하기 위한 노력의 일환으로 추진되었다. 특히 수백억 달러 규모의 컴퓨팅 자원으로 훈련되는 최첨단 AI 모델들이 사이버 공격, 대량살상무기 개발, 중요 인프라 파괴 등 심각한 사회적 피해를 야기할 가능성에 대한 선제적 대응이 이 법안 추진의 주요 동기이다.

2. 규제 요지와 적용대상

2.1. 규제 요지

이 법의 핵심은 대규모 AI 모델 개발자에게 사전 예방적 안전 관리 체계 구축을 의무화하는 것이다. 개발자는 모델 훈련 시작 전부터 포괄적인 안전보안 프로토콜을 수립하고, 정기적인 위험성 평가와 제3자 감사를 받아야 한다.

또한, 임계적 피해(Critical Harm) 개념을 도입하여 ①화학·생물학·방사능·핵무기의 생성이나 사용으로 인한 대량 사상자, ②중요 인프라에 대한 사이버공격으로 인한 대량 사상자나 5억 달러 이상의 손해, ③제한적 인간 감독 하에서 AI가 수행하는 범죄적 행위로 인한 대량 사상자나 5억 달러 이상의 손해, ④법무장관이 결정한 비교 가능한 심각성의 공공 안전에 대한 중대한 피해 등을 야기할 수 있는 AI 모델의 상업적 사용을 엄격히 제한한다.

이 외에도 내부 고발자 보호 조항을 통해 AI 기업 내부에서 안전 문제를 제기할 수 있는 환경을 조성하고, 투명성 의무를 통해 공중이 AI 안전 정보에 접근할 수 있도록 보장하고자 한다.

2.2. 적용 대상

이 법의 규제대상모델(Covered Model)은 대규모 AI모델에 한정된다. 대규모 AI모델은 ①초기 훈련 시 10^{26} FLOPS 이상의 컴퓨팅 파워를 사용하고 비용이 1억 달러를 초과하는 모델 또는 ②기존 규제대상모델을 3×10^{25} FLOPS 이상으로 파인튜닝하여 비용이 1천만 달러를 초과하는 모델로 정의된다. 이러한 임계값은 주 정부 장관에 의해 매년 인플레이션에 따라 조정될 예정이다.

적용 주체는 규제대상모델의 초기 훈련을 수행하는 개발자, 초당 100기가비트를 초과하는 데이터센터 네트워킹으로 연결되고 최소 10^{20} FLOPS의 이론적 최대 컴퓨팅 용량을 가진 컴퓨팅 클러스터 운영자, 제3의 독립적인 조사관, 그리고 개발자의 직원, 계약업체, 하도급업체 등이다.

적용 대상 예외조항으로는 연방정부 기관과의 계약 조건과 엄격히 충돌하는 경우, 모델 훈련이나 주/연방법 준수를 위한 합리적 평가 목적으로만 사용하는 경우 등이 있다.

3. AI 혁신 신탁기금의 재정 조성 및 지원

이 법안은 매사추세츠 주를 AI 혁신의 중심지로 성장시키기 위해 'AI 혁신 신탁기금'을 설립하여 AI 산업 발전을 지원하는 내용을 담고 있다. 주 경제개발부 장관이 수탁자가 되며, 매사추세츠 기술공원공사의 전무이사와 협의하여 ①핵심 산업 부문에서 AI 모델을 개발하거나 배포하는 회사들에게 보조금 또는 기타 재정 지원 제공, ②AI 기업가정신 프로그램의 설립 또는 촉진,

③AI 연구에 대한 보조금 또는 기타 재정 지원 제공 등의 목적으로 기금을 사용하는 형태이다.

기금의 수입원은 ①주 의회가 승인하고 기금에 입금되도록 특별히 지정한 모든 세출예산 또는 기타 자금, ②기금 내 모든 자금에서 발생한 이자, ③외부로부터 받은 기타 보조금, 장려금, 기부금, 상환금 또는 기타 기여금 등으로 구성된다. 기금에 입금된 금액은 추가 세출예산 없이 지출될 수 있으며, 회계연도 말 잔액은 일반기금으로 환수되지 않고 다음 연도로 이월된다.

4. 세부 규제 내용

4.1. 개발단계의 사전적 책무

개발자는 규제대상모델 훈련을 시작하기 전에 포괄적인 안전 인프라를 구축해야 한다. 이러한 사전 준비 체계는 크게 보안 인프라 구축, 안전보안 프로토콜 수립, 그리고 지속적 관리 체계 마련으로 구성된다.

보안 인프라 구축 측면에서 개발자는 고도 지속 위협을 포함한 정교한 행위자로부터 무단 접근, 오용, 안전하지 않은 사후 훈련 수정을 방지하는 합리적인 관리적·기술적·물리적 사이버보안 보호조치를 구현해야 한다. 이와 함께 모델 훈련, 운영 및 모든 파생형에 대해 신속하게 완전 차단을 실행할 수 있는 능력을 구현하여 위기 상황 시 즉각적인 대응이 가능하도록 해야 한다.

안전보안 프로토콜 수립은 이 법안의 핵심 요구사항 중 하나로, 임계적 피해를 야기할 불합리한 위험을 피하기 위한 서면의 별도 프로토콜을 마련해야 한다. 이 프로토콜은 단순한 지침서가 아니라 실질적인 안전 관리를 위한 종합적 체계로서, 성공적으로 구현된다면 임계적 피해 위험을 제기하는 모델 생산을 방지할 보호조치 및 절차를 명시해야 한다. 특히 객관적이고 구체적인 준수 요구사항을 명시하여 개발자나 제3자가 쉽게 준수 여부를 확인할 수 있도록 해야 하며, 위험성 평가를 위한 테스트 절차와 사후 훈련 수정 위험 평가 방법도 상세히 기술해야 한다. 또한 완전 차단 조건과 의무 이행 방법, 안전장치 구현 방법을 포함하되, 특히 중요 인프라 중단 위험을 고려한 완전 차단 조건과 프로토콜 수정 절차까지 포괄적으로 다뤄야 한다.

지속적 관리 체계 마련을 위해서는 고위 인력을 지정하여 안전보안 프로토콜이 서면대로 구현되도록 보장하는 거버넌스 체계를 구축해야 한다. 이는 단순한 문서화를 넘어서 실질적인 실행력을 담보하기 위한 조치다. 동시에 안전보안 프로토콜의 편집되지 않은 사본을 상업적 사용 중단 후 5년 이상 보관하여 장기적 추적 관리가 가능하도록 해야 하며, 모델 능력 변화와 업계 모범사례를 고려한 연간 검토를 통해 프로토콜의 지속적 개선을 도모해야 한다. 투명성 확보를 위해 편집된 프로토콜을 공개하고 법무장관에게 전달해야 하며, 실질적 수정 시에는 30일 이내 업데이트를 통해 실시간 정보 공유를 보장해야 한다. 이 모든 체계는 임계적 피해의 불합리한 위험을 방지하기 위한 기타 적절한 조치와 함께 종합적인 안전 관리 생태계를 구성한다.

사전적 책무	핵심 보안활동
사이버보안 및 안전인프라 구축 의무	- 고도 지속 위협을 포함한 정교한 행위자로부터 무단 접근, 오용, 안전하지 않은 사후 훈련 수정을 방지하는 합리적인 관리적·기술적·물리적 사이버보안 보호조치를 구현 - 위기 상황시 신속하게 완전 차단을 실행할 수 있는 능력을 구현
안전보안 프로토콜 수립	- 임계적 피해를 야기할 불합리한 위험 예방을 위한 별도 안전보안 프로토콜 수립(문서화 필요) * 준수 요구사항, 위험성 평가를 위한 테스트 절차, 사후 훈련 수정 위험 평가 방법, 완전 차단 조건 등 포함 - 프로토콜 공개 및 주 법무장관에게 제출 의무, 실질적 수정시 30일 이내에 업데이트 책임 부과
지속적 관리 체계 마련	- 제3자의 독립적인 조사관을 통한 내부 통제체계 및 노력에 관한 평가조사보고서 작성 · 제출 · 공개 · 보관(5년) 의무 - 연간 준수 명세서 제출 의무

4.2. 개발자의 배포 및 유지 단계 의무

규제대상모델의 실제 배포와 운영 단계에서 개발자는 보다 엄격한 검증과 지속적 모니터링 체계를 구축해야 한다. 이 단계의 의무는 크게 배포 전 안전성 검증, 지속적 모니터링 및 보고, 그리고 위험 관리로 구분된다.

배포 전 안전성 검증 과정에서 개발자는 모델을 상업적·공개적 용도로 사용하거나 배포하기 전에 임계적 피해를 야기할 합리적 능력이 있는지에 대한 종합적 평가를 실시해야 한다. 이러한 평가는 단순한 형식적 절차가 아니라 제3자가 복제할 수 있을 정도로 상세한 테스트 결과를 기록하고 5년간 보관하여 검증 가능성을 담보해야 한다. 평가 결과를 바탕으로 임계적 피해를 방지하는 적절한 안전장치를 구현해야 하며, 모델의 행동과 그로 인한 피해를 정확하고 신뢰성 있게 추적할 수 있는 시스템을 구축해야 한다.

지속적 모니터링 및 보고 체계는 AI 모델의 동적 특성을 고려한 핵심 안전 장치다. 개발자는 규제대상모델이나 파생형이 임계적 피해를 야기할 불합리한 위험이 있는 경우 상업적·공개적 사용을 즉시 중단해야 하며, 매년 절차, 정책, 보호조치, 능력 및 안전장치에 대한 종합적 재평가를 통해 변화하는 위험 환경에 대응해야 한다. 특히 AI 안전사고가 발생하거나 그 가능성을 인지한 경우 72시간 이내에 법무장관에게 신고하여 신속한 대응이 가능하도록 해야 한다.

제3자 검증 시스템은 객관적이고 독립적인 안전성 평가를 위한 핵심 장치로, 개발자는 매년 독립적인 제3자 조사관을 고용하여 법률 요구사항 준수에 대한 심층적 조사를 받아야 한다. 조사관은 개발자의 준수 조치에 대한 상세한 평가와 함께 위반 사례 및 개선 권고사항을 제시하

고, 내부 통제 체계에 대한 종합적 평가를 통해 시스템 차원의 개선점을 도출해야 한다. 이러한 조사 결과는 수석 조사관의 서명이 포함된 조사보고서 형태로 문서화되며, 편집된 보고서는 공개하고 법무장관에게 전달하되 편집되지 않은 원본은 5년간 보관하여 추후 검증이 가능하도록 해야 한다.

최고 경영진의 책임성 확보를 위해 최고기술책임자 또는 그보다 상급 임원이 서명한 연간 준수 명세서를 법무장관에게 제출해야 한다. 이 명세서는 임계적 피해의 성격과 규모에 대한 평가, 안전보안 프로토콜 준수 부족 위험에 대한 분석, 그리고 준수 검증 과정에 대한 상세한 설명을 포함해야 한다. 특히 최초 사용 또는 배포 후 30일 이내 제출을 통해 초기 배포 단계에서의 안전성을 즉시 확인할 수 있도록 하며, 이후 매년 제출을 통해 지속적인 모니터링 체계를 유지해야 한다.

배포 및 유지단계	핵심 보안활동
지속적 모니터링 및 보고 체계	– 임계적 피해를 야기할 불합리한 위험이 있는 경우 상업적·공개적 사용을 즉시 중단 – 매년 절차, 정책, 보호조치, 능력 및 안전장치에 대한 종합적 재평가를 통해 변화하는 위험 환경에 대응 – AI 안전사고가 발생하거나 그 가능성을 인지한 경우 72시간 이내에 법무장관에게 신고
제3자 검증시스템 구축	– 제3자의 독립적인 조사관을 통한 내부 통제체계 및 노력에 관한 평가조사보고서 작성 · 제출 · 공개 · 보관(5년) 의무
책임성 확보	– 연간 준수 명세서 제출 의무

4.3 컴퓨팅 클러스터 운영자의 의무

컴퓨팅 클러스터 운영자는 AI 생태계의 게이트키퍼 역할을 담당하며, 대규모 AI 모델 훈련의 첫 번째 방어선으로서 중요한 책임을 진다. 이들의 의무는 고객 식별 및 모니터링, 기록 관리, 그리고 위험 대응 능력 구축으로 구성된다.

고객 식별 및 모니터링 측면에서 클러스터 운영자는 고객이 규제대상모델 훈련에 충분한 컴퓨트 자원을 활용할 때 포괄적인 정보 수집과 평가를 수행해야 한다. 이는 금융기관의 고객 확인(Know Your Customer, KYC) 절차와 유사한 접근법으로, 고객의 기본 식별정보인 신원, 결제수단, 연락처뿐만 아니라 사업목적과 규제대상모델 훈련 의도까지 파악해야 한다. 특히 반복적으로 대규모 컴퓨트 자원을 이용하는 고객에 대해서는 매번 기본 정보를 재검증하고 훈련 의도를 재평가하여 지속적인 모니터링 체계를 유지해야 한다.

기록 관리 및 투명성 확보를 위해 IP 주소와 접근 기록을 포함한 모든 활동 기록을 체계적으로 보관해야 한다. 이러한 기록들은 7년간 보관되어야 하며, 법무장관의 요청이 있을 경우 즉시

제공할 수 있도록 준비되어야 한다. 이는 AI 모델 훈련 과정의 추적 가능성을 확보하고 사후 조사나 감독 시 필요한 정보를 제공하기 위한 중요한 조치다.

위험 대응 능력 구축을 위해서는 고객의 통제 하에 있는 규제대상모델 훈련이나 운영에 사용되는 모든 자원에 대해 신속한 완전 차단을 실행할 수 있는 능력을 구현해야 한다. 이는 위험 상황 발생 시 즉각적인 대응을 통해 피해 확산을 방지하기 위한 핵심 안전장치다.

클러스터 운영자는 또한 국가표준기술연구소, 미국 인공지능 안전 연구소 등 신뢰할 만한 표준설정 기관의 업계 모범사례와 지침을 적극적으로 고려해야 한다. 동시에 개인정보 보호와 보안 요구 사이의 균형을 위해 불필요한 개인정보 수집을 방지하고, 기업 연락처 정보 활용을 통해 개인정보 노출 위험을 최소화할 수 있다.

4.4 사후적 신고관리 의무(내부고발자 보호체계)

이 법안의 독특한 특징 중 하나는 AI 분야에 특화된 포괄적인 내부고발자 보호 체계를 구축한다는 점이다. 이 체계는 AI 기술의 특수성을 고려하여 전통적인 내부고발자 보호를 넘어서는 확장된 보호 범위와 다층적 신고 시스템을 제공한다.

보호 범위의 확장에서 주목할 점은 직원의 정의를 무보수 자문관과 기업 임원까지 포함하도록 광범위하게 설정했다는 것이다. 이는 AI 개발 과정에서 다양한 형태로 참여하는 전문가들을 모두 보호 대상에 포함시키려는 의도로 해석된다. 보호되는 신고 내용 역시 이 법률의 직접적인 위반뿐만 아니라 규제대상모델이 아닌 모든 AI 모델의 임계적 피해 위험까지 포괄하여, 법적 요구사항을 넘어서는 예방적 접근을 보여준다. 또한 안전보안 프로토콜과 관련된 허위진술 신고도 보호 대상에 포함시켜 정보의 투명성과 정확성을 확보하고자 한다.

금지행위와 구제 수단은 포괄적이면서도 실질적인 보호를 제공한다. 법무장관 등 공공기관에 대한 신고 방해와 신고자에 대한 어떤 형태의 보복도 엄격히 금지하며, 안전보안 프로토콜 관련 기만적 진술 역시 금지 대상에 포함된다. 피해를 입은 직원은 기존 내부고발자 보호법에 따라 법원에 구제를 신청할 수 있어 실질적인 구제 수단이 보장된다.

내부 신고 시스템의 구축은 이 법안의 핵심적인 안전 장치 중 하나다. 개발자는 규제대상모델 관련 업무에 종사하는 모든 직원, 계약업체, 하도급업체가 법률 위반, 허위진술, 알려진 위험 미공개 등에 대해 익명으로 신고할 수 있는 합리적인 내부 프로세스를 구축해야 한다. 이러한 신고에 대해서는 반드시 조사를 수행해야 하며, 신고자에게 최소 월별로 조사 진행상황과 대응 조치에 대한 업데이트를 제공하여 신고의 실효성을 보장해야 한다. 모든 신고와 대응 기록은 7년간 보관되어야 하며, 분기별로 관련되지 않은 임원진에게 보고하여 조직 차원의 투명성을 확보해야 한다.

직원 권리 보장과 공익적 활용을 위해 개발자는 게시판 방식 또는 연간 서면 고지 중 하나를 선택하여 원격 근무자를 포함한 모든 직원에게 권리와 책임을 명확히 고지해야 한다. 법무장관이나 국장은 공익을 위해 필요하다고 판단할 경우 기밀정보를 편집한 후 고발 내용을 공개할 수

있어, 개별 사안을 넘어서는 시스템적 문제에 대한 사회적 인식 제고도 가능하다. 이러한 포괄적 보호 체계는 AI 기업 내부에서 자발적인 안전 문화를 조성하고, 외부 규제만으로는 발견하기 어려운 위험 요소들을 사전에 식별할 수 있게 하는 중요한 안전망 역할을 한다.

5. 정책적 시사점

매사추세츠 주 AI 안전법은 미국 주 차원에서 대규모 AI 모델에 대한 포괄적 규제 체계를 구축하려는 선도적 시도로 평가된다. 이 법안의 통과 여부와 실제 시행 결과는 다른 주들의 유사한 입법에 중요한 선례가 될 것이다.

특히 임계적 피해 개념의 도입과 단계별 의무 체계는 AI 개발의 전체 생명주기에 걸친 안전 관리를 가능하게 한다는 점에서 의미가 크다. 제3자 검증과 투명성 의무를 통한 객관적 평가 시스템, 그리고 내부고발자 보호를 통한 자율적 안전 문화 조성은 규제의 실효성을 높이는 중요한 장치들이다.

다만 매년 제3자 조사, 안전보안 프로토콜 수립 및 유지, 72시간 내 신고 체계 구축 등에 소요되는 비용이 상당하기 때문에, 이러한 규제가 '경쟁촉진'의 의도와 달리 AI 개발자들에게 상당한 준수 비용과 운영상 부담을 가할 것으로 예상된다. 유사 법안인 「캘리포니아 SB1047」이 주지사 거부권 행사로 폐지된 이유도 이러한 우려 때문이었다. 「캘리포니아 SB1047」은 모델 훈련과정에서 위험을 사전 평가하고 필요시 중단시킬 수 있는 '킬 스위치' 기능을 의무화하는 내용이 포함되어 있었다.

향후 미국 주 정부의 AI 규제법안들은 혁신과 안전 사이의 적절한 균형점을 찾는 것이 향후 과제가 될 것이다. 또한 연방정부 차원의 AI 규제와의 조화, 다른 주와의 규제 일관성 확보 등도 중요한 고려사항이다.

현재 매사추세츠 주 AI 법안은 심의 중인 상황으로 최종 제정 가능성은 불확실하다. 그러나, 이 법안이 제시하는 AI 거버넌스 모델이 타 기술중심 주들의 AI규제 법안들이 추구하는 방향성과 유사하다는 점에서, 향후 주 의회 중심의 AI 규제 입법에 상당한 영향을 미칠 것으로 전망된다.

참고문헌

법률 초안 원문
https://trackbill.com/bill/massachusetts-senate-bill-37-an-act-promoting-economic-development-with-emerging-artificial-intelligence-models-and-safety/2688754/

Multistate (2025). Artificial Intelligence (AI) Legislation,
https://www.multistate.ai/artificial-intelligence-ai-legislation

별첨. 미국 매사추세츠주, 「인공지능모델과 안전성을 통한 경제발전촉진법(안)」 핵심 조항

* 하단의 번역은 참고용으로 정확한 법적 해석은 원문 확인 필요.

원 문	번 역 문
SECTION 1. Chapter 29 of the General Laws is hereby amended by adding the following new section:-	제1조. 일반법 제29장을 다음의 새로운 조항을 추가하여개정한다:-
Section 2GGGGGG. Artificial Intelligence Innovation Trust Fund (a) There shall be established and set up on the books of the commonwealth a separate fund to be known as the Massachusetts Artificial Intelligence Innovation Trust Fund. The secretary of economic development shall be the trustee of the fund and shall, in consultation with the executive director of the Massachusetts Technology Park Corporation established pursuant to chapter 40J, expend money from the fund to: (i) provide grants or other financial assistance to companies developing or deploying artificial intelligence models in key industry sectors as enumerated in line 7002-8070 of section 2 of chapter 238 of the Acts of 2024; provided, however, that the secretary may seek the commitment of matching or other additional funds from private sources before making an expenditure from the fund; (ii) establishment or promotion of artificial intelligence entrepreneurship programs, which may include partnerships with research institutions in the commonwealth or other entrepreneur support organizations; or (iii) provide grants or other financial assistance for research in artificial intelligence through or in partnership with the Massachusetts Technology Park Corporation.	제2GGGGGG조. 인공지능 혁신 신탁기금 (a) 연방의 장부에 매사추세츠 인공지능 혁신 신탁기금으로 알려질 별도의 기금을 설립하고 설치한다. 경제개발부 장관은 기금의 수탁자가 되며, 제 40J장에 따라 설립된 매사추세츠 기술공원공사의 전무이사와 협의하여 다음의 목적으로 기금에서 지출한다: (i) 2024년 법률 제238장 제2조 7002-8070항에 열거된 핵심 산업 부문에서 인공지능 모델을 개발하거나 배포하는 회사들에게 보조금 또는 기타재정지원을 제공하고; 단, 장관은 기금에서 지출하기 전에 민간 출처로부터 대응자금 또는 기타 추가 자금의 약속을 구할 수 있다; (ii) 연방 내 연구기관 또는 기타 기업가 지원 조직과의 파트너십을 포함할 수 있는 인공지능 기업가정신 프로그램의 설립 또는 촉진; 또는 (iii) 매사추세츠 기술공원공사를 통해 또는 이와 파트너십을 맺어 인공지능 연구에 대한 보조금 또는기타 재정지원제공.
(b) There shall be credited to the fund an amount equal to: (i) any appropriations or other money authorized by the general court and specifically designated to be credited to the fund; (ii) interest earned on any money in the fund; and (iii) any other grants, premiums, gifts, reimbursements or other contributions received by the commonwealth from any source for or in support of the purposes described in subsection (a).	(b) 기금에는 다음과 같은 금액이 입금되어야 한다: (i) 총회가 승인하고 기금에 입금되도록 특별히 지정한 모든 세출예산 또는 기타 자금; (ii) 기금 내 모든 자금에서 발생한 이자; 그리고 (iii) 제(a)항에 기술된 목적을 위해 또는 이를 지원하기 위해 연방이 모든 출처로부터 받은 기타 보조금, 장려금, 기부금, 상환금 또는 기타 기여금.
(c) Amounts credited to the fund may be expended without further appropriation. For the purpose of accommodating timing discrepancies between the	(c) 기금에 입금된 금액은 추가 세출예산 없이 지출될 수 있다. 수입 접수와 관련 지출 간의 시기적 불일치를 수용하기 위해, 기금은 비용을 발생시킬 수 있으며, 감사관은 주 회계

receipt of revenues and related expenditures, the fund may incur expenses, and the comptroller shall certify for payment, amounts not to exceed the most recent revenue estimate as certified by the secretary of elder affairs, as reported in the state accounting system. Any money remaining in the fund at the end of a fiscal year shall not revert to the General Fund and shall be available for expenditure in a subsequent fiscal year.	시스템에 보고된 바에 따라 노인복지부 장관이 인증한 가장 최근의 수입 추정치를 초과하지 않는 금액에 대해 지불을 인증해야 한다. 회계연도 말에 기금에 남아있는 모든 자금은 일반기금으로 환수되지 않으며 후속 회계연도에 지출할 수 있다.
SECTION 2. The General Laws are hereby amended by inserting after chapter 93L the following new chapter:-	제2조. 일반법을 제93L장 다음에 다음의 새로운 장을 삽입하여 개정한다:-
CHAPTER 93M. Artificial Intelligence Models	제93M장. 인공지능 모델
Section 1. As used in this chapter, the following terms shall have the following meanings unless the context clearly requires otherwise:	제1조. 이 장에서 사용되는 다음 용어들은 문맥상 달리 요구되지 않는 한 다음의 의미를 갖는다:
"Advanced persistent threat", an adversary with sophisticated levels of expertise and significant resources that allow it, through the use of multiple different attack vectors including, but not limited to, cyber, physical or deception, to generate opportunities to achieve objectives including, but not limited to, (i) establishing or extending its presence within the information technology infrastructure of an organization for the purpose of exfiltrating information; (ii) undermining or impeding critical aspects of a mission, program or organization; or (iii) placing itself in a position to do so in the future.	"고도 지속 위협"이란 사이버, 물리적 또는 기만을 포함하되 이에 국한되지 않는 다양한 공격 벡터의 사용을 통해 다음을 포함하되 이에 국한되지 않는 목표를 달성할 기회를 창출할 수 있도록 하는 정교한 수준의 전문성과 상당한 자원을 가진 적대자를 말한다: (i) 정보 유출 목적으로 조직의 정보기술 인프라 내에서 자신의 존재를 확립하거나 확장하는 것; (ii) 임무, 프로그램 또는 조직의 중요한 측면을 훼손하거나 방해하는 것; 또는 (iii) 향후 그렇게 할 수 있는 위치에 자신을 두는 것.
"Artificial intelligence", an engineered or machine-based system that varies in its level of autonomy and which may, for explicit or implicit objectives, infer from the input it receives how to generate outputs that may influence physical or virtual environments	"인공지능"이란 자율성 수준이 다양하며, 명시적 또는 묵시적 목표를 위해 받은 입력으로부터 물리적 또는 가상 환경에 영향을 미칠 수 있는 출력을 생성하는 방법을 추론할 수 있는 엔지니어링되거나 기계 기반의 시스템을 말한다
"Artificial intelligence safety incident", an incident that demonstrably increases the risk of a critical harm occurring by means of: (i) A covered model or covered model derivative autonomously engaging in behavior other than at the request of a user; (ii) Theft, misappropriation, malicious use, inadvertent release, unauthorized access or escape of the model weights of a covered model or covered model derivative; (iii) The critical failure of technical or administrative controls, including controls limiting the ability to modify a covered model or covered model derivative; or (iv) Unauthorized use of a covered model or covered model derivative to cause or materially enable critical harm.	"인공지능 안전 사고"란 다음의 수단으로 임계적 피해가 발생할 위험을 명백히 증가시키는 사고를 말한다: (i) 규제대상모델 또는 규제대상모델 파생형이 사용자의 요청이 아닌 자율적으로 행동에 관여하는 것; (ii) 규제대상모델 또는 규제대상모델 파생형의 모델 가중치의 도난, 오용, 악의적 사용, 부주의한 유출, 무단 접근 또는 탈취; (iii) 규제대상모델 또는 규제대상모델 파생형을 수정할 능력을 제한하는 통제를 포함한 기술적 또는 관리적 통제의 심각한 실패; 또는 (iv) 임계적 피해를 야기하거나 실질적으로 가능하게 하기 위한 규제대상모델 또는 규제대상모델 파생형의 무단 사용.
"Computing cluster", a set of machines transitively connected by data center networking of over 100	"컴퓨팅 클러스터"란 초당 100기가비트를 초과하는 데이터센터 네트워킹으로 이행적으로 연결된 머신 세트로서,

gigabits per second that has a theoretical maximum computing capacity of at least 10^{20} integer or floating-point operations per second and can be used for training artificial intelligence.	최소 초당 10^{20}개의 정수 또는 부동소수점 연산의 이론적 최대 컴퓨팅 용량을 가지며 인공지능 훈련에 사용될 수 있는 것을 말한다.
"Covered model", an artificial intelligence model which is: (i) trained using a quantity of computing power greater than 10^{26} integer or floating-point operations, the cost of which exceeds $100,000,000 when calculated using the average market prices of cloud compute at the start of training as reasonably assessed by the developer; or (ii) created by fine-tuning a covered model using a quantity of computing power equal to or greater than 3 times 10^{25} integer or floating-point operations, the cost of which, as reasonably assessed by the developer, exceeds $10,000,000 if calculated using the average market price of cloud compute at the start of fine-tuning; provided, however, that investment thresholds established pursuant to this section shall be adjusted for inflation annually, not later than January 31, by the growth rate of the inflation index over the preceding 12 months; and provided further, that the inflation index shall consist of the per cent change in inflation as measured by the per cent change in the consumer price index for all urban consumers for the Boston metropolitan area as determined by the bureau of labor statistics of the United States department of labor.	"규제대상모델"이란 다음과 같은 인공지능 모델을 말한다: (i) 개발자가 합리적으로 평가한 바에 따라 훈련 시작 시 클라우드 컴퓨트의 평균 시장 가격을 사용하여 계산했을 때 비용이 100,000,000달러를 초과하는, 10^{26}개를 초과하는 정수 또는 부동소수점 연산의 컴퓨팅 파워를 사용하여 훈련된 모델; 또는 (ii) 파인튜닝 시작 시 클라우드 컴퓨트의 평균 시장 가격을 사용하여 계산했을 때 개발자가 합리적으로 평가한 바에 따라 비용이 10,000,000달러를 초과하는, 3×10^{25}개 이상의 정수 또는 부동소수점 연산과 같거나 그보다 큰 컴퓨팅 파워의 양을 사용하여 규제대상모델을 파인튜닝하여 생성된 모델; 단, 이 조항에 따라 설정된 투자 임계값은 선행 12개월 동안의 인플레이션 지수 증가율에 의해 매년 1월 31일까지 인플레이션에 맞추어 조정되어야 한다; 그리고 또한, 인플레이션 지수는 미국 노동부 노동통계청이 결정한 보스턴 대도시권의 모든 도시 소비자를 위한 소비자물가지수의 백분율 변화로 측정되는 인플레이션의 백분율 변화로 구성되어야 한다.
"Covered model derivative", a copy of a covered model that: (i) is unmodified; (ii) has been subjected to post-training modifications related to fine-tuning; (iii) has been fine- tuned using a quantity of computing power not exceeding 3 times 1025 or floating point operations, the cost of which, as reasonably assessed by the developer, exceeds $10,000,000 if calculated using the average market price of cloud compute at the start of fine-tuning; or (iv) has been combined with other software.	"규제대상모델 파생형"이란 다음 중 하나에 해당하는 규제대상모델의 사본을 말한다: (i) 수정되지 않은 것; (ii) 파인튜닝과 관련된 사후 훈련 수정을 받은 것; (iii) 파인튜닝 시작 시 클라우드 컴퓨트의 평균 시장 가격을 사용하여 계산했을 때 개발자가 합리적으로 평가한 바에 따라 비용이 10,000,000달러를 초과하는, 3×10^{25}개 이하의 정수 또는 부동소수점 연산의 컴퓨팅 파워를 사용하여 파인튜닝된 것; 또는 (iv) 다른 소프트웨어와 결합된 것.
"Critical harm", a harm caused or materially enabled by a covered model or covered model derivative including: (i) the creation or use in a manner that results in mass casualties of a chemical, biological, radiological or nuclear weapon; (ii) mass casualties or at least $500,000,000 of damage resulting from cyberattacks on critical infrastructure by a model conducting, or providing precise instructions for conducting, a cyberattack or	"임계적 피해"란 규제대상모델 또는 규제대상모델 파생형에 의해 야기되거나 실질적으로 가능하게 된 피해로서 다음을 포함한다: (i) 대량 사상자를 초래하는 방식으로 화학, 생물학, 방사능 또는 핵무기의 생성 또는 사용; (ii) 중요 인프라에 대한 사이버공격을 수행하거나 중요 인프라에 대한 사이버공격 또는 일련의 사이버공격 수행을 위한 정확한 지시를 제공하는 모델에 의해 발생하는 대량 사상자 또는 최소 500,000,000달러의 손해;

series of cyberattacks on critical infrastructure; (iii) mass casualties or at least $500,000,000 of damage resulting from an artificial intelligence model engaging in conduct that: (A) acts with limited human oversight, intervention or supervision; and (B) results in death, great bodily injury, property damage or property loss, and would, if committed by a human, constitute a crime specified in any general or special law that requires intent, recklessness or gross negligence, or the solicitation or aiding and abetting of such a crime; or (iv) other grave harms to public safety that are of comparable severity to the harms described herein as determined by the attorney general; provided, however, that "critical harm" shall not include: (i) harms caused or materially enabled by information that a covered model or covered model derivative outputs if the information is otherwise reasonably publicly accessible by an ordinary person from sources other than a covered model or covered model derivative; (ii) harms caused or materially enabled by a covered model combined with other software, including other models, if the covered model did not materially contribute to the other software’s ability to cause or materially enable the harm; or (iii) harms that are not caused or materially enabled by the developer’s creation, storage, use or release of a covered model or covered model derivative; provided further, that monetary harm thresholds established pursuant to this section shall be adjusted for inflation annually, not later than January 31, by the growth rate of the inflation index over the preceding 12 months; and provided further, that the inflation index shall consist of the per cent change in inflation as measured by the per cent change in the consumer price index for all urban consumers for the Boston metropolitan area as determined by the bureau of labor statistics of the United States department of labor.	(iii) 다음과 같은 행위에 관여하는 인공지능 모델로부터 발생하는 대량 사상자 또는 최소 500,000,000달러의 손해: (A) 제한적인 인간의 감독, 개입 또는 지도 하에 행동하고; (B) 사망, 중상해, 재산 손해 또는 재산 손실을 초래하며, 인간이 저질렀다면 고의, 무모함 또는 중과실을 요구하는 일반법 또는 특별법에 명시된 범죄, 또는 그러한 범죄의 교사 또는 방조를 구성할 행위; (iv) 법무장관이 결정한 바에 따라 여기에 설명된 피해와 비교할 만한 심각성을 갖는 공공 안전에 대한 기타 중대한 피해; 단, "임계적 피해"는 다음을 포함하지 않는다: (i) 해당 정보가 규제대상모델 또는 규제대상모델 파생형이 아닌 다른 출처로부터 일반인이 합리적으로 공개적으로 접근할 수 있는 경우, 규제대상모델 또는 규제대상모델 파생형이 출력하는 정보에 의해 야기되거나 실질적으로 가능하게 된 피해; (ii) 규제대상모델이 다른 소프트웨어의 피해 야기 또는 실질적 가능 능력에 실질적으로 기여하지 않은 경우, 다른 모델을 포함한 다른 소프트웨어와 결합된 규제대상모델에 의해 야기되거나 실질적으로 가능하게 된 피해; (iii) 개발자의 규제대상모델 또는 규제대상모델 파생형의 생성, 저장, 사용 또는 출시에 의해 야기되거나 실질적으로 가능하게 되지 않은 피해; 또한, 이 조항에 따라 설정된 금전적 피해 임계값은 선행 12개월 동안의 인플레이션 지수 증가율에 의해 매년 1월 31일까지 인플레이션에 맞추어 조정되어야 한다; 그리고 또한, 인플레이션 지수는 미국 노동부 노동통계청이 결정한 보스턴 대도시권의 모든 도시 소비자를 위한 소비자물가지수의 백분율 변화로 측정되는 인플레이션의 백분율 변화로 구성되어야 한다.
"Critical infrastructure", assets, systems and networks, whether physical or virtual, the incapacitation or destruction of which would have a debilitating effect on physical security, economic security, public health or safety in the commonwealth.	"중요 인프라"란 물리적이든 가상적이든, 그 무력화 또는 파괴가 연방의 물리적 보안, 경제적 보안, 공중 보건 또는 안전에 쇠약하게 하는 영향을 미칠 자산, 시스템 및 네트워크를 말한다.
"Developer", a person that performs the initial training of a covered model by: (i) training a model using a sufficient quantity of computing power and cost; or (ii) fine-tuning an existing covered model or covered model derivative using a quantity of computing power	"개발자"란 다음에 의해 규제대상모델의 초기 훈련을 수행하는 자를 말한다: (i) 충분한 양의 컴퓨팅 파워와 비용을 사용하여 모델을 훈련시키는 것; 또는 (ii) 규제대상모델로 분류되기에 충분한 양의 컴퓨팅 파워와 비용을 사용하여 기존의 규제대상모델 또는 규제대상모델 파생형을

and cost sufficient to qualify as a covered model.	파인튜닝하는 것.
"Fine-tuning", adjusting the model weights of a trained covered model or covered model derivative by exposing such model to additional data.	"파인튜닝"이란 훈련된 규제대상모델 또는 규제대상모델 파생형을 추가 데이터에 노출시켜 해당 모델의 모델 가중치를 조정하는 것을 말한다.
"Full shutdown", the cessation of operation of: (i) the training of a covered model; (ii) a covered model controlled by a developer; and (iii) all covered model derivatives controlled by a developer.	"완전 차단"이란 다음의 운영 중단을 말한다: (i) 규제대상모델의 훈련; (ii) 개발자가 통제하는 규제대상모델; 그리고 (iii) 개발자가 통제하는 모든 규제대상모델 파생형.
"Model weight", a numerical parameter in an artificial intelligence model that is adjusted through training and that helps determine how inputs are transformed into outputs.	"모델 가중치"란 인공지능 모델 내의 수치적 매개변수로서 훈련을 통해 조정되며 입력이 출력으로 변환되는 방식을 결정하는 데 도움이 되는 것을 말한다.
"Person", an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee or any other nongovernmental organization or group of persons acting in concert.	"자(개인)"란 개인, 개인사업체, 회사, 파트너십, 합작투자, 신디케이트, 사업신탁, 기업, 법인, 유한책임회사, 협회, 위원회 또는 공동으로 행동하는 기타 비정부 조직이나 개인 집단을 말한다.
"Post-training modification", modifying the capabilities of a covered model or covered model derivative by any means including, but not limited to, fine-tuning, providing such model with access to tools or data, removing safeguards against hazardous misuse or misbehavior of such model or combining such model with, or integrating such model into, other software.	"사후 훈련 수정"이란 파인튜닝, 그러한 모델에 도구나 데이터에 대한 접근 제공, 그러한 모델의 위험한 오용이나 오작동에 대한 안전장치 제거, 그러한 모델을 다른 소프트웨어와 결합하거나 다른 소프트웨어에 통합하는 것을 포함하되 이에 국한되지 않는 모든 수단으로 규제대상모델 또는 규제대상모델 파생형의 능력을 수정하는 것을 말한다.
"Safety and security protocol", documented technical and organizational protocols that: (i) are used to manage the risks of developing and operating covered models or covered model derivatives across their life cycle, including risks posed by causing or enabling or potentially causing or enabling the creation of covered model derivatives; and (ii) specify that compliance with such protocols is required in order to train, operate, possess or provide external access to the developer’s covered model or covered model derivatives.	"안전보안 프로토콜"이란 다음과 같은 문서화된 기술적 및 조직적 프로토콜을 말한다: (i) 규제대상모델 파생형의 생성을 야기하거나 가능하게 하거나 잠재적으로 야기하거나 가능하게 함으로써 제기되는 위험을 포함하여 규제대상모델 또는 규제대상모델 파생형의 생명주기 전반에 걸친 개발 및 운영 위험을 관리하는 데 사용되는 것; 그리고 (ii) 개발자의 규제대상모델 또는 규제대상모델 파생형을 훈련, 운영, 보유 또는 외부 접근을 제공하기 위해서는 그러한 프로토콜의 준수가 요구된다고 명시하는 것.
"Secretary", the secretary of technology services and security.	"장관"이란 기술서비스보안부 장관을 말한다.
Section 2. (a) Before beginning to train a covered model, a developer shall: (1) implement reasonable administrative, technical and physical cybersecurity protections to prevent unauthorized access to, misuse of or unsafe post-training modifications of the covered model and all covered model derivatives controlled by the developer that are appropriate in light of the risks associated with the covered model, including from advanced persistent threats or other sophisticated actors; (2) implement the capability to promptly enact a full	제2조. (a) 규제대상모델 훈련을 시작하기 전에 개발자는 다음을 수행해야 한다: (1) 고도 지속 위협 또는 기타 정교한 행위자를 포함하여 규제대상모델과 관련된 위험에 비추어 적절한, 개발자가 통제하는 규제대상모델 및 모든 규제대상모델 파생형에 대한 무단 접근, 오용 또는 안전하지 않은 사후 훈련 수정을 방지하기 위한 합리적인 관리적, 기술적 및 물리적 사이버보안 보호조치를 구현; (2) 신속하게 완전 차단을 실행할 수 있는 능력을 구현;

shutdown;	
(3) implement a written and separate safety and security protocol that:	(3) 다음을 포함하는 서면의 별도 안전보안 프로토콜을 구현:
(A) specifies protections and procedures that, if successfully implemented, would comply with the developer's duty to take reasonable care to avoid producing a covered model or covered model derivative that poses an unreasonable risk of causing or materially enabling a critical harm;	(A) 성공적으로 구현된다면 임계적 피해를 야기하거나 실질적으로 가능하게 할 불합리한 위험을 제기하는 규제대상모델 또는 규제대상모델 파생형을 생산하는 것을 피하기 위해 합리적 주의를 기울일 개발자의 의무를 준수할 보호조치 및 절차를 명시;
(B) states compliance requirements in an objective manner and with sufficient detail and specificity to allow the developer or a third party to readily ascertain whether the requirements of the safety and security protocol have been followed;	(B) 개발자 또는 제3자가 안전보안 프로토콜의 요구사항이 준수되었는지 쉽게 확인할 수 있도록 객관적인 방식으로 그리고 충분한 세부사항과 구체성을 가지고 준수 요구사항을 명시;
(C) identifies a testing procedure which takes safeguards into account as appropriate to reasonably evaluate if a covered model poses a substantial risk of causing or enabling a critical harm and if any covered model derivatives pose a substantial risk of causing or enabling a critical harm;	(C) 규제대상모델이 임계적 피해를 야기하거나 가능하게 할 상당한 위험을 제기하는지 그리고 모든 규제대상모델 파생형이 임계적 피해를 야기하거나 가능하게 할 상당한 위험을 제기하는지 합리적으로 평가하기 위해 적절하게 안전장치를 고려하는 테스트 절차를 식별;
(D) describes in detail how the testing procedure assesses the risks associated with post-training modifications;	(D) 테스트 절차가 사후 훈련 수정과 관련된 위험을 어떻게 평가하는지 상세히 기술;
(E) describes in detail how the testing procedure addresses the possibility that a covered model or covered model derivative may be used to make post-training modifications or create another covered model in a manner that may cause or materially enable a critical harm;	(E) 테스트 절차가 규제대상모델 또는 규제대상모델 파생형이 임계적 피해를 야기하거나 실질적으로 가능하게 할 수 있는 방식으로 사후 훈련 수정을 하거나 다른 규제대상모델을 생성하는 데 사용될 가능성을 어떻게 다루는지 상세히 기술;
(F) describes in detail how the developer will fulfill their obligations under this chapter;	(F) 개발자가 이 장 하에서의 의무를 어떻게 이행할 것인지 상세히 기술;
(G) describes in detail how the developer intends to implement any safeguards and requirements referenced in this section;	(G) 개발자가 이 조항에서 언급된 모든 안전장치와 요구사항을 어떻게 구현할 의도인지 상세히 기술;
(H) describes in detail the conditions under which a developer would enact a full shutdown account for, as appropriate, the risk that a shutdown of the covered model, or particular covered model derivatives, may cause disruptions to critical infrastructure;	(H) 규제대상모델 또는 특정 규제대상모델 파생형의 차단이 중요 인프라에 대한 중단을 야기할 수 있는 위험을 적절히 고려하여 개발자가 완전 차단을 실행할 조건을 상세히 기술;
and (I) describes in detail the procedure by which the safety and security protocol may be modified;	그리고 (I) 안전보안 프로토콜이 수정될 수 있는 절차를 상세히 기술;
(4) ensure that the safety and security protocol is implemented as written, including by designating senior personnel to be responsible for ensuring compliance by employees and contractors working on a covered model or any covered model derivatives controlled by the developer, monitoring and reporting on implementation;	(4) 규제대상모델 또는 개발자가 통제하는 모든 규제대상모델 파생형에 작업하는 직원과 계약업체의 준수를 보장할 책임이 있는 고위 인력을 지정하고, 구현을 모니터링하고 보고하는 것을 포함하여 안전보안 프로토콜이 서면대로 구현되도록 보장;
(5) retain an unredacted copy of the safety and	(5) 모든 업데이트나 개정의 기록과 날짜를 포함하여

security protocol for not less than 5 years after the covered model is no longer made available for commercial, public or foreseeably public use, including records and dates of any updates or revisions;	규제대상모델이 더 이상 상업적, 공개적 또는 예견 가능한 공개 사용에 제공되지 않은 후 5년 이상 안전보안 프로토콜의 편집되지 않은 사본을 보관;
(6) conduct an annual review of the safety and security protocol to account for any changes to the capabilities of the covered model and industry best practices and, if necessary, make modifications to such policy;	(6) 규제대상모델의 능력 변화와 업계 모범사례를 고려하여 안전보안 프로토콜의 연간 검토를 수행하고, 필요한 경우 그러한 정책을 수정;
(7) conspicuously publish a redacted copy of the safety and security protocol and transmit a copy of said redacted safety and security protocol to the attorney general;	(7) 안전보안 프로토콜의 편집된 사본을 눈에 띄게 공개하고 상기 편집된 안전보안 프로토콜의 사본을 법무장관에게 전달;
provided, however, that a redaction in the safety and security protocol may be made only if the redaction is reasonably necessary to protect public safety, trade secrets as defined in section 2 of chapter 93 or confidential information pursuant to any general, special or federal law;	단, 안전보안 프로토콜의 편집은 공공 안전, 제93장 제2조에 정의된 영업비밀 또는 일반법, 특별법 또는 연방법에 따른 기밀정보를 보호하기 위해 합리적으로 필요한 경우에만 할 수 있다;
provided further, that the developer shall grant to the attorney general access to the unredacted safety and security protocol upon request;	또한, 개발자는 요청 시 법무장관에게 편집되지 않은 안전보안 프로토콜에 대한 접근을 허가해야 한다;
provided further, that a safety and security protocol disclosed to the attorney general shall not be a public record for the purposes of chapter 66;	또한, 법무장관에게 공개된 안전보안 프로토콜은 제66장의 목적상 공공기록이 아니다;
and provided further, that if the safety and security protocol is materially modified, the developer shall conspicuously publish and transmit to the attorney general an updated redacted copy of such protocol within 30 days of the modification;	그리고 또한, 안전보안 프로토콜이 실질적으로 수정된 경우, 개발자는 수정 후 30일 이내에 그러한 프로토콜의 업데이트된 편집된 사본을 눈에 띄게 공개하고 법무장관에게 전달해야 한다;
and (8) take reasonable care to implement other appropriate measures to prevent covered models and covered model derivatives from posing unreasonable risks of causing or materially enabling critical harms.	그리고 (8) 규제대상모델과 규제대상모델 파생형이 임계적 피해를 야기하거나 실질적으로 가능하게 할 불합리한 위험을 제기하지 않도록 방지하기 위해 기타 적절한 조치를 구현하는 데 합리적 주의를 기울인다.
(b) Before using a covered model or covered model derivative for a purpose not exclusively related to the training or reasonable evaluation of the covered model for compliance with state or federal law or before making a covered model or covered model derivative available for commercial, public or foreseeably public use, the developer of a covered model shall:	(b) 주법 또는 연방법 준수를 위한 규제대상모델의 훈련이나 합리적 평가와 배타적으로 관련되지 않은 목적으로 규제대상모델 또는 규제대상모델 파생형을 사용하기 전에 또는 규제대상모델 또는 규제대상모델 파생형을 상업적, 공개적 또는 예견 가능한 공개 사용에 제공하기 전에 규제대상모델의 개발자는 다음을 수행해야 한다:
(i) assess whether the covered model is reasonably capable of causing or materially enabling a critical harm;	(i) 규제대상모델이 임계적 피해를 야기하거나 실질적으로 가능하게 할 합리적 능력이 있는지 평가;
(ii) record, as and when reasonably possible, and retain for not less than 5 years after the covered model is no longer made available for commercial, public or foreseeably public use, information on any specific tests and test results used in said assessment which	(ii) 합리적으로 가능한 한, 상기 평가에 사용된 모든 특정 테스트와 테스트 결과에 대한 정보로서 제3자가 테스트 절차를 복제할 수 있을 정도로 충분한 세부사항을 제공하는 정보를 기록하고, 규제대상모델이 더 이상 상업적, 공개적 또는 예견 가능한 공개 사용에 제공되지 않은 후 5년 이상

provides sufficient detail for third parties to replicate the testing procedure;	보관;
(iii) take reasonable care to implement appropriate safeguards to prevent the covered model and covered model derivatives from causing or materially enabling a critical harm;	(iii) 규제대상모델과 규제대상모델 파생형이 임계적 피해를 야기하거나 실질적으로 가능하게 하는 것을 방지하기 위해 적절한 안전장치를 구현하는 데 합리적 주의를 기울임;
and (iv) take reasonable care to ensure, to the extent reasonably possible, that the covered model's actions and the actions of covered model derivatives, as well as critical harms resulting from their actions, may be accurately and reliably attributed to such model or model derivative.	그리고 (iv) 합리적으로 가능한 범위에서 규제대상모델의 행동과 규제대상모델 파생형의 행동, 그리고 그들의 행동으로부터 발생하는 임계적 피해가 그러한 모델 또는 모델 파생형에 정확하고 신뢰성 있게 귀속될 수 있도록 보장하는 데 합리적 주의를 기울임.
(c) A developer shall not use a covered model or covered model derivative for a purpose not exclusively related to the training or reasonable evaluation of the covered model for compliance with state or federal law or make a covered model or a covered model derivative available for commercial, public or foreseeably public use if there is an unreasonable risk that the covered model or covered model derivative will cause or materially enable a critical harm.	(c) 개발자는 규제대상모델 또는 규제대상모델 파생형이 임계적 피해를 야기하거나 실질적으로 가능하게 할 불합리한 위험이 있는 경우, 주법 또는 연방법 준수를 위한 규제대상모델의 훈련이나 합리적 평가와 배타적으로 관련되지 않은 목적으로 규제대상모델 또는 규제대상모델 파생형을 사용하거나 규제대상모델 또는 규제대상모델 파생형을 상업적, 공개적 또는 예견 가능한 공개 사용에 제공해서는 안 된다.
(d) A developer of a covered model shall annually reevaluate the procedures, policies, protections, capabilities and safeguards implemented pursuant to this section.	(d) 규제대상모델의 개발자는 이 조항에 따라 구현된 절차, 정책, 보호조치, 능력 및 안전장치를 매년 재평가해야 한다.
(e)(1) A developer of a covered model shall annually retain a third-party investigator that conducts investigations consistent with best practices for investigators to perform an independent investigation of compliance with the requirements of this section;	(e)(1) 규제대상모델의 개발자는 이 조항의 요구사항 준수에 대한 독립적인 조사를 수행하기 위해 조사관의 모범사례와 일치하는 조사를 수행하는 제3자 조사관을 매년 고용해야 한다;
provided, however, that an investigator shall conduct investigations consistent with regulations issued by the secretary pursuant to section 7.	단, 조사관은 제7조에 따라 장관이 발행한 규정과 일치하는 조사를 수행해야 한다.
The investigator shall be granted access to unredacted materials as necessary to comply with the investigator's obligations contained herein.	조사관은 여기에 포함된 조사관의 의무를 준수하는 데 필요한 편집되지 않은 자료에 대한 접근을 허가받아야 한다.
The investigator shall produce an investigation report including, but not limited to:	조사관은 다음을 포함하되 이에 국한되지 않는 조사보고서를 작성해야 한다:
(i) a detailed assessment of the developer's steps to comply with the requirements of this section;	(i) 이 조항의 요구사항을 준수하기 위한 개발자의 조치에 대한 상세한 평가;
(ii) if applicable, any identified instances of noncompliance with the requirements of this section and any recommendations for how the developer can improve its policies and processes for ensuring compliance with the requirements of this section;	(ii) 해당하는 경우, 이 조항의 요구사항 미준수로 식별된 모든 사례와 개발자가 이 조항의 요구사항 준수를 보장하기 위한 정책과 프로세스를 어떻게 개선할 수 있는지에 대한 권고사항;
(iii) a detailed assessment of the developer's internal controls, including designation and empowerment of senior personnel responsible for ensuring compliance	(iii) 개발자와 그 직원이나 계약업체의 준수를 보장할 책임이 있는 고위 인력의 지정과 권한 부여를 포함한 개발자의 내부 통제에 대한 상세한 평가;

by the developer and any employees or contractors thereof;	
and (iv) the signature of the lead investigator certifying the results contained within the investigation report;	그리고 (iv) 조사보고서에 포함된 결과를 인증하는 수석 조사관의 서명;
and provided further, that the investigator shall not knowingly make a material misrepresentation in said report.	그리고 또한, 조사관은 상기 보고서에서 고의로 실질적인 허위진술을 해서는 안 된다.
(2) The developer shall retain an unredacted copy of the investigation report for not less than 5 years after the covered model is no longer made available for commercial, public or foreseeably public use.	(2) 개발자는 규제대상모델이 더 이상 상업적, 공개적 또는 예견 가능한 공개 사용에 제공되지 않은 후 5년 이상 조사보고서의 편집되지 않은 사본을 보관해야 한다.
The developer shall conspicuously publish a redacted copy of the investigator's report and transmit to the attorney general a redacted copy of the investigator's report;	개발자는 조사관의 보고서의 편집된 사본을 눈에 띄게 공개하고 법무장관에게 조사관의 보고서의 편집된 사본을 전달해야 한다;
provided, however, that a redaction in the investigator's report may be made only if the redaction is reasonably necessary to protect public safety, trade secrets as defined in section 2 of chapter 93 or confidential information pursuant to state and federal law;	단, 조사관의 보고서의 편집은 공공 안전, 제93장 제2조에 정의된 영업비밀 또는 주법과 연방법에 따른 기밀정보를 보호하기 위해 합리적으로 필요한 경우에만 할 수 있다;
provided further, that the developer shall grant to the attorney general access to the unredacted investigator's report upon request;	또한, 개발자는 요청 시 법무장관에게 편집되지 않은 조사관의 보고서에 대한 접근을 허가해야 한다;
and provided further, that an investigator's report disclosed to the attorney general shall not be a public record for the purposes of chapter 66.	그리고 또한, 법무장관에게 공개된 조사관의 보고서는 제66장의 목적상 공공기록이 아니다.
(f)(1) A developer of a covered model shall annually, until such time that the covered model and any covered model derivatives controlled by the developer cease to be in or available for commercial or public use, submit to the attorney general a statement of compliance signed by the chief technology officer, or a more senior corporate officer, that shall specify or provide, at a minimum:	(f)(1) 규제대상모델의 개발자는 개발자가 통제하는 규제대상모델과 모든 규제대상모델 파생형이 상업적 또는 공개적 사용에 있거나 이용 가능하지 않게 될 때까지 매년 최고기술책임자 또는 더 상급의 기업 임원이 서명한 준수 명세서를 법무장관에게 제출해야 하며, 이는 최소한 다음을 명시하거나 제공해야 한다:
(i) an assessment of the nature and magnitude of critical harms that the covered model or covered model derivatives may reasonably cause or materially enable and the outcome of the assessment required by subsection (b);	(i) 규제대상모델 또는 규제대상모델 파생형이 합리적으로 야기하거나 실질적으로 가능하게 할 수 있는 임계적 피해의 성격과 규모에 대한 평가 및 제(b)항에 의해 요구되는 평가의 결과;
(ii) an assessment of the risk that compliance with the safety and security protocol may be insufficient to prevent the covered model or covered model derivatives from causing or materially enabling critical harms;	(ii) 안전보안 프로토콜의 준수가 규제대상모델 또는 규제대상모델 파생형이 임계적 피해를 야기하거나 실질적으로 가능하게 하는 것을 방지하기에 불충분할 수 있는 위험에 대한 평가;
and (iii) a description of the process used by the signing officer to verify compliance with the requirements of this section, including a description of the materials reviewed by the signing officer, a description of testing or other evaluation performed to support the statement and the contact information of	그리고 (iii) 서명 임원이 검토한 자료의 설명, 명세서를 뒷받침하기 위해 수행된 테스트 또는 기타 평가에 대한 설명, 준수를 검증하기 위해 의존한 제3자의 연락처 정보를 포함하여 서명 임원이 이 조항의 요구사항 준수를 검증하기 위해 사용한 프로세스에 대한 설명.

any third parties relied upon to validate compliance. (2) A developer shall submit such statement to the attorney general not later than 30 days after using a covered model or covered model derivative for a purpose not exclusively related to the training or reasonable evaluation of the covered model for compliance with state or federal law or making a covered model or covered model derivative available for commercial, public or foreseeably public use; provided, however, that no such initial statement shall be required for a covered model derivative if the developer submitted a compliant initial statement and any applicable annual statements for the covered model from which the covered model derivative is derived. (g) A developer of a covered model shall report each artificial intelligence safety incident affecting the covered model or any covered model derivatives controlled by the developer to the attorney general within 72 hours of the developer learning of the artificial intelligence safety incident or facts sufficient to establish a reasonable belief that an artificial intelligence safety incident has occurred. (h) This section shall apply to the development, use or commercial or public release of a covered model or covered model derivative for any use that is not the subject of a contract with a federal government entity, even if that covered model or covered model derivative was developed, trained or used by a federal government entity; provided, however, that this section shall not apply to a product or service to the extent that compliance would strictly conflict with the terms of a contract between a federal government entity and the developer of a covered model.	(2) 개발자는 주법 또는 연방법 준수를 위한 규제대상모델의 훈련이나 합리적 평가와 배타적으로 관련되지 않은 목적으로 규제대상모델 또는 규제대상모델 파생형을 사용하거나 규제대상모델 또는 규제대상모델 파생형을 상업적, 공개적 또는 예견 가능한 공개 사용에 제공한 후 30일 이내에 그러한 명세서를 법무장관에게 제출해야 한다; 단, 개발자가 규제대상모델 파생형이 파생된 규제대상모델에 대해 준수하는 초기 명세서와 해당하는 연간 명세서를 제출한 경우 규제대상모델 파생형에 대해서는 그러한 초기 명세서가 요구되지 않는다. (g) 규제대상모델의 개발자는 개발자가 통제하는 규제대상모델 또는 모든 규제대상모델 파생형에 영향을 미치는 각 인공지능 안전사고를 개발자가 인공지능 안전사고를 알게 되거나 인공지능 안전사고가 발생했다는 합리적 믿음을 확립하기에 충분한 사실을 알게 된 후 72시간 이내에 법무장관에게 신고해야 한다. (h) 이 조항은 규제대상모델 또는 규제대상모델 파생형이 연방정부 기관에 의해 개발, 훈련 또는 사용되었더라도 연방정부 기관과의 계약 대상이 아닌 모든 용도를 위한 규제대상모델 또는 규제대상모델 파생형의 개발, 사용 또는 상업적 또는 공개적 출시에 적용된다; 단, 이 조항은 준수가 연방정부 기관과 규제대상모델의 개발자 간의 계약 조건과 엄격히 충돌하는 범위에서는 제품이나 서비스에 적용되지 않는다.
Section 3. (a) (1) A person that operates a computing cluster shall implement written policies and procedures to do all of the following when a customer utilizes compute resources which would be sufficient to train a covered model: (i) obtain the prospective customer's basic identifying information and business purpose for utilizing the computing cluster including, but not limited to: (A) the identity of the prospective customer; (B) the means and source of payment, including any associated financial institution, credit card number, account number, customer identifier, transaction identifiers or virtual currency wallet or wallet address identifier;	제3조. (a) (1) 컴퓨팅 클러스터를 운영하는 자는 고객이 규제대상모델을 훈련시키기에 충분한 컴퓨트 자원을 활용할 때 다음의 모든 사항을 수행하기 위한 서면 정책 및 절차를 구현해야 한다: (i) 다음을 포함하되 이에 국한되지 않는 잠재 고객의 기본 식별 정보 및 컴퓨팅 클러스터 활용의 사업 목적을 획득: (A) 잠재 고객의 신원; (B) 관련 금융기관, 신용카드 번호, 계좌 번호, 고객 식별자, 거래 식별자 또는 가상화폐 지갑 또는 지갑 주소 식별자를 포함한 지불 수단 및 출처;

and (C) the email address and telephone number used to verify the prospective customer's identity; (ii) assess whether the prospective customer intends to utilize the computing cluster to train a covered model; (iii) retain any internet protocol addresses used by the customer for access or administration and the date and time of each access or administrative action; (iv) maintain for not less than 7 years, and provide to the attorney general upon request, appropriate records of actions taken under this section, including policies and procedures put into effect; (v) implement the capability to promptly enact a full shutdown of any resources being used to train or operate a covered model under the customer's control. (2) If a customer repeatedly utilizes computer resources that would be sufficient to train a covered model, the operator of the computer cluster shall validate said basic identifying information and assess whether such customer intends to utilize the computing cluster to train a covered model prior to each utilization. (b) A person that operates a computing cluster shall consider industry best practices and applicable guidance from the National Institute of Standards and Technology, including the United States Artificial Intelligence Safety Institute, and other reputable standard-setting organizations. (c) In complying with the requirements of this section, a person that operates a computing cluster may impose reasonable requirements on customers to prevent the collection or retention of personal information that the person operating such computing cluster would not otherwise collect or retain, including a requirement that a corporate customer submit corporate contact information rather than information that would identify a specific individual.	그리고 (C) 잠재 고객의 신원을 확인하는 데 사용되는 이메일 주소 및 전화번호; (ii) 잠재 고객이 규제대상모델을 훈련시키기 위해 컴퓨팅 클러스터를 활용할 의도가 있는지 평가; (iii) 고객이 접근 또는 관리를 위해 사용한 모든 인터넷 프로토콜 주소와 각 접근 또는 관리 행위의 날짜 및 시간을 보관; (iv) 시행된 정책 및 절차를 포함하여 이 조항에 따라 취해진 조치의 적절한 기록을 7년 이상 유지하고, 요청 시 법무장관에게 제공; (v) 고객의 통제 하에 있는 규제대상모델을 훈련시키거나 운영하는 데 사용되는 모든 자원의 신속한 완전 차단을 실행할 수 있는 능력을 구현. (2) 고객이 규제대상모델을 훈련시키기에 충분한 컴퓨터 자원을 반복적으로 활용하는 경우, 컴퓨터 클러스터의 운영자는 각 활용 이전에 상기 기본 식별 정보를 검증하고 그러한 고객이 규제대상모델을 훈련시키기 위해 컴퓨팅 클러스터를 활용할 의도가 있는지 평가해야 한다. (b) 컴퓨팅 클러스터를 운영하는 자는 미국 인공지능 안전 연구소를 포함한 국가표준기술연구소의 업계 모범사례 및 적용 가능한 지침, 그리고 기타 신뢰할 만한 표준설정 기관의 지침을 고려해야 한다. (c) 이 조항의 요구사항을 준수함에 있어, 컴퓨팅 클러스터를 운영하는 자는 기업 고객이 특정 개인을 식별할 정보보다는 기업 연락처 정보를 제출하도록 요구하는 것을 포함하여, 그러한 컴퓨팅 클러스터를 운영하는 자가 달리 수집하거나 보관하지 않을 개인정보의 수집 또는 보관을 방지하기 위해 고객에게 합리적인 요구사항을 부과할 수 있다.
Section 4. (a) (1) The attorney general shall have the authority to enforce the provisions of this chapter. Except as provided in section 5, nothing in this chapter shall be construed as creating a new private right of action or serving as the basis for a private right of action that would not otherwise have had a basis under any other law but for the enactment of this chapter. (2) The attorney general may initiate a civil action in the superior court against an entity in the name of the commonwealth or as parens patriae on behalf of individuals for a violation of this chapter. The attorney	제4조. (a) (1) 법무장관은 이 장의 조항을 집행할 권한을 갖는다. 제5조에 규정된 경우를 제외하고, 이 장의 어떤 내용도 새로운 사적 소송권을 창설하거나 이 장의 제정이 없었다면 다른 법률 하에서 근거를 갖지 못했을 사적 소송권의 기초가 되는 것으로 해석되어서는 안 된다. (2) 법무장관은 이 장의 위반에 대해 연방의 명의로 또는 개인들을 대리하여 고등법원에서 기관을 상대로 민사소송을 제기할 수 있다. 법무장관은 다음을 구할 수 있다:

general may seek:	
(i) against a developer of a covered model or covered model derivative for a violation that causes death or bodily harm to another human, harm to property, theft or misappropriation of property, or that constitutes an imminent risk or threat to public safety that occurs on or after January 1, 2026, a civil penalty in an amount not exceeding:	(i) 2026년 1월 1일 이후에 발생하는 다른 인간에게 사망 또는 신체적 피해, 재산에 대한 피해, 재산의 도난 또는 오용을 야기하거나 공공 안전에 대한 급박한 위험 또는 위협을 구성하는 위반에 대해 규제대상모델 또는 규제대상모델 파생형의 개발자에게 다음을 초과하지 않는 금액의 민사처벌:
(A) for a first violation, 5 per cent of the cost of the quantity of computing power used to train the covered model to be calculated using the average market prices of cloud compute at the time of training;	(A) 첫 번째 위반의 경우, 훈련 시 클라우드 컴퓨트의 평균 시장 가격을 사용하여 계산될 규제대상모델 훈련에 사용된 컴퓨팅 파워 양의 비용의 5퍼센트;
or (B) for any subsequent violation, 15 percent of the cost of the quantity of computing power used to train the covered model as calculated herein;	또는 (B) 후속 위반의 경우, 여기에 계산된 바와 같이 규제대상모델 훈련에 사용된 컴퓨팅 파워 양의 비용의 15퍼센트;
(b) In determining whether a developer exercised reasonable care in the creation, use or deployment of a covered model or covered model derivative, the attorney general shall consider:	(b) 개발자가 규제대상모델 또는 규제대상모델 파생형의 생성, 사용 또는 배포에서 합리적 주의를 기울였는지 판단함에 있어, 법무장관은 다음을 고려해야 한다:
(i) the quality of such developer's safety and security protocol;	(i) 그러한 개발자의 안전보안 프로토콜의 품질;
(ii) the extent to which the developer faithfully implemented and followed its safety and security protocol;	(ii) 개발자가 자신의 안전보안 프로토콜을 충실히 구현하고 준수한 정도;
(iii) whether, in quality and implementation, the developer's safety and security protocol was comparable to those of developers of models trained using a comparable amount of compute resources;	(iii) 품질과 구현에 있어서 개발자의 안전보안 프로토콜이 비교 가능한 양의 컴퓨트 자원을 사용하여 훈련된 모델의 개발자들의 것과 비교할 만했는지 여부;
(iv) the quality and rigor of the developer's investigation, documentation, evaluation and management of risks of critical harm posed by its model.	(iv) 자신의 모델이 제기하는 임계적 피해 위험에 대한 개발자의 조사, 문서화, 평가 및 관리의 품질과 엄격성.
(c) (1) A provision within a contract or agreement that seeks to waive, preclude or burden the enforcement of a liability arising from a violation of this chapter, or to shift such liability to any person or entity in exchange for their use or access of, or right to use or access, a developer's product or services, including by means of a contract or adhesion, shall be deemed to be against public policy and void.	(c) (1) 이 장의 위반으로 발생하는 책임의 집행을 면제, 배제 또는 부담시키거나, 개발자의 제품 또는 서비스의 사용이나 접근, 또는 사용이나 접근할 권리와 교환하여 그러한 책임을 다른 자나 기관에게 전가하려고 하는 계약 또는 협정 내의 조항은 부착계약을 통한 것을 포함하여 공공정책에 반하는 것으로 간주되고 무효가 된다.
(2) Notwithstanding any corporate formalities, the court shall impose joint and several liability on affiliated entities for purposes of effectuating the intent of this section to the maximum extent permitted by law if the court concludes that:	(2) 모든 기업상의 형식에도 불구하고, 법원이 다음과 같이 결론지을 경우 이 조항의 의도를 법이 허용하는 최대 범위까지 실현하기 위한 목적으로 계열 기업들에 대해 연대책임을 부과해야 한다:
(i) the affiliated entities, in the development of the corporate structure among such affiliated entities, took steps to purposely and unreasonably limit or	(i) 계열 기업들이 그러한 계열 기업들 간의 기업 구조를 발전시킴에 있어 고의적이고 불합리하게 책임을 제한하거나 회피하기 위한 조치를 취했고; 그리고

avoid liability; and (ii) as a result of any such steps, the corporate structure of the developer or affiliated entities would frustrate recovery of penalties, damages, or injunctive relief under this section. (d) Penalties collected pursuant to this section by the attorney general shall be deposited into the General Fund and subject to appropriation.	(ii) 그러한 조치들의 결과로, 개발자나 계열 기업들의 기업 구조가 이 조항 하에서 처벌금, 손해배상 또는 금지명령 구제의 회복을 좌절시킬 것인 경우. (d) 이 조항에 따라 법무장관이 징수한 처벌금은 일반기금에 예치되고 세출예산의 대상이 된다.
Section 5. (a) For purposes of this section, the following words shall have the following meanings unless the context clearly requires otherwise: "Contractor or subcontractor", a firm, corporation, partnership or association and its responsible managing officer, as well as any supervisors, managers or officers found by the attorney general or director to be personally and substantially responsible for the rights and responsibilities of employees under this chapter. "Director", the director of the department of labor standards as established under section 1 of chapter 23. "Employee", any person who performs services for wages or salary under a contract of employment, express or implied, for an employer, including: (i) contractors or subcontractors and unpaid advisors involved with assessing, managing or addressing the risk of critical harm from covered models or covered model derivatives; and (ii) corporate officers. "Public body" shall have the same meaning as ascribed to it in section 185 of chapter 149. (b) A developer of a covered model or a contractor or subcontractor of the developer shall not: (i) prevent an employee from disclosing information to the attorney general or any other public body, including through terms and conditions of employment or seeking to enforce terms and conditions of employment, if the employee has reasonable cause to believe the information indicates that: (A) the developer is out of compliance with the requirements of this chapter; or (B) an artificial intelligence model, including a model that is not a covered model or a covered model derivative, poses an unreasonable risk of causing or materially enabling critical harm, even if the employer is not out of compliance with any state or federal law; (ii) retaliate against an employee for disclosing such	제5조. (a) 이 조항의 목적상, 다음 단어들은 문맥상 달리 명확히 요구되지 않는 한 다음의 의미를 갖는다: "계약업체 또는 하도급업체"란 회사, 법인, 파트너십 또는 협회 및 그 책임 관리 임원뿐만 아니라 법무장관 또는 국장이 이 장 하에서 직원의 권리와 책임에 대해 개인적이고 실질적으로 책임이 있다고 판단한 모든 감독자, 관리자 또는 임원을 말한다. "국장"이란 제23장 제1조에 따라 설립된 노동기준부의 국장을 말한다. "직원"이란 명시적이든 묵시적이든 고용계약에 따라 고용주를 위해 임금 또는 급여를 받고 서비스를 수행하는 모든 자를 말하며, 다음을 포함한다: (i) 규제대상모델 또는 규제대상모델 파생형으로부터의 임계적 피해 위험을 평가, 관리 또는 대처하는 데 관여하는 계약업체 또는 하도급업체 및 무보수 자문관; 그리고 (ii) 기업 임원. "공공기관"은 제149장 제185조에 규정된 것과 동일한 의미를 갖는다. (b) 규제대상모델의 개발자 또는 개발자의 계약업체 또는 하도급업체는 다음을 하여서는 안 된다: (i) 직원이 다음을 나타낸다고 믿을 합리적인 근거가 있는 정보인 경우, 고용 조건을 통해 또는 고용 조건을 강제하려고 시도하는 것을 포함하여 직원이 법무장관 또는 기타 공공기관에 정보를 공개하는 것을 방지: (A) 개발자가 이 장의 요구사항을 준수하지 않고 있다는 것; 또는 (B) 규제대상모델 또는 규제대상모델 파생형이 아닌 모델을 포함한 인공지능 모델이 고용주가 주법 또는 연방법을 위반하지 않더라도 임계적 피해를 야기하거나 실질적으로 가능하게 할 불합리한 위험을 제기한다는 것; (ii) 그러한 정보를 법무장관 또는 기타 공공기관에 공개한

information to the attorney general or any other public body; or	직원에 대해 보복; 또는
(iii) make false or materially misleading statements related to its safety and security protocol in any manner that would constitute an unfair or deceptive trade practice under chapter 93A.	(iii) 제93A장에 따른 불공정하거나 기만적인 거래 관행을 구성할 방식으로 안전보안 프로토콜과 관련하여 허위이거나 실질적으로 오해를 불러일으키는 진술을 하는 것.
(d) The attorney general or director may publicly release or provide to the governor any complaint, or a summary of such complaint, filed pursuant to this section if the attorney general or director concludes that doing so will serve the public interest; provided, however, that any information that is confidential, otherwise exempt from the provisions of chapter 66, qualifies as a trade secret under sections 42 to 42G, inclusive, of chapter 93 or is determined by the attorney general or director to likely pose an unreasonable risk to public safety if disclosed shall be redacted from the complaint prior to disclosure.	(d) 법무장관 또는 국장은 그렇게 하는 것이 공익에 도움이 될 것이라고 결론지을 경우 이 조항에 따라 제기된 고발 또는 그러한 고발의 요약을 공개적으로 발표하거나 주지사에게 제공할 수 있다; 단, 기밀인 정보, 제66장의 규정에서 달리 면제되는 정보, 제93장 제42조부터 제42G조까지에 따른 영업비밀에 해당하는 정보 또는 법무장관이나 국장이 공개될 경우 공공 안전에 불합리한 위험을 제기할 가능성이 있다고 판단한 정보는 공개 전에 고발서에서 편집되어야 한다.
(e) A developer shall provide a clear notice to all employees working on covered models and covered model derivatives of their rights and responsibilities under this section, including the rights of employees of contractors and subcontractors to utilize the developer's internal process for making protected disclosures pursuant to subsection (f).	(e) 개발자는 제(f)항에 따른 보호된 공개를 위해 개발자의 내부 프로세스를 활용할 계약업체 및 하도급업체 직원의 권리를 포함하여 이 조항 하에서의 권리와 책임에 대해 규제대상모델 및 규제대상모델 파생형에 작업하는 모든 직원에게 명확한 고지를 제공해야 한다.
A developer is presumed to be in compliance with the requirements of this subsection if the developer:	개발자가 다음을 수행하는 경우 이 항의 요구사항을 준수하는 것으로 추정된다:
(i) at all times posts and displays within all workplaces maintained by the developer a notice to all employees of their rights and responsibilities under this section, ensures that all new employees receive equivalent notice and ensures that employees who work remotely periodically receive an equivalent notice; or	(i) 개발자가 유지하는 모든 직장 내에 이 조항 하에서의 모든 직원의 권리와 책임에 대한 고지를 항상 게시하고 표시하며, 모든 신규 직원이 동등한 고지를 받도록 보장하고 원격 근무하는 직원이 정기적으로 동등한 고지를 받도록 보장; 또는
(ii) at least annually, provides written notice to all employees of their rights and responsibilities under this chapter and ensures that such notice is received and acknowledged by all of those employees.	(ii) 최소한 매년, 이 장 하에서의 권리와 책임에 대해 모든 직원에게 서면 고지를 제공하고 그러한 고지가 모든 해당 직원에 의해 수령되고 승인되도록 보장.
(f) (1) A developer shall provide a reasonable internal process through which an employee, contractor, subcontractor or employee of a contractor or subcontractor working on a covered model or covered model derivative may anonymously disclose information to the developer if the employee believes, in good faith, that the developer has violated any provision of this chapter or any other general or special law, has made false or materially	(f) (1) 개발자는 규제대상모델 또는 규제대상모델 파생형에 작업하는 직원, 계약업체, 하도급업체 또는 계약업체나 하도급업체의 직원이 개발자가 이 장의 조항 또는 기타 일반법이나 특별법의 조항을 위반했거나, 안전보안 프로토콜과 관련하여 허위이거나 실질적으로 오해를 불러일으키는 진술을 했거나, 직원들에게 알려진 위험을 공개하지 않았다고 선의로 믿는 경우 개발자에게 익명으로 정보를 공개할 수 있는 합리적인 내부 프로세스를 제공해야 한다.

misleading statements related to its safety and security protocol or has failed to disclose known risks to employees.	
The developer shall conduct an investigation related to any information disclosed through such process and provide, at a minimum, a monthly update to the person who made the disclosure regarding the status of the developer's investigation of the disclosure and the actions taken by the developer in response to the disclosure.	개발자는 그러한 프로세스를 통해 공개된 모든 정보와 관련하여 조사를 수행하고, 최소한 공개자에게 개발자의 공개 조사 상황 및 공개에 대응하여 개발자가 취한 조치에 관하여 월별 업데이트를 제공해야 한다.
(2) Any disclosure and response created pursuant to this subsection shall be maintained for not less than 7 years from the date when the disclosure or response is created.	(2) 이 항에 따라 생성된 모든 공개 및 대응은 공개 또는 대응이 생성된 날로부터 7년 이상 유지되어야 한다.
Each disclosure and response shall be shared with officers and directors of the developer whose acts or omissions are not implicated by the disclosure or response not less than once per quarter.	각 공개 및 대응은 공개 또는 대응에 의해 연루되지 않은 개발자의 임원 및 이사들과 분기당 최소 한 번 공유되어야 한다.
In the case of a report or disclosure regarding alleged misconduct by a contractor or subcontractor, the developer shall notify the officers and directors of the contractor or subcontractor whose acts or omissions are not implicated by the disclosure or response about the status of their investigation not less than once per quarter.	계약업체 또는 하도급업체의 혐의 위반행위에 관한 보고 또는 공개의 경우, 개발자는 공개 또는 대응에 의해 연루되지 않은 계약업체 또는 하도급업체의 임원 및 이사들에게 그들의 조사 상황에 대해 분기당 최소 한 번 통지해야 한다.
(g) This section shall not be construed to limit any rights or obligations of employees under section 185 of chapter 149 or any other state or federal law.	(g) 이 조항은 제149장 제185조 또는 기타 주법이나 연방법 하에서 직원의 권리나 의무를 제한하는 것으로 해석되어서는 안 된다.