



제418회 국회 (정기회)
제1차 행정안전위원회

전자정부법 일부개정법률안

검 토 보 고

〈헌법기관을 포함한 국가기관의 사이버안보 및
정보시스템 등의 장애예방·대응 체계 강화〉
■ 유상범의원 대표발의(의안번호 제2200674호)

2024. 9.

행 정 안 전 위 원 회

수석전문위원 유상조

목 차

I . 제안경위	1
II . 제안이유 및 주요내용	1
III . 검토의견	3
1. 헌법기관을 포함한 국가기관의 사이버안보 체계 강화 (안 제56조제4항 삭제)	6
2. 헌법기관을 포함한 국가기관의 정보시스템 등의 장애예방·대응 체계 강화(안 제56조의2제1항, 제2항~제6항 신설 등)	10
3. 개정안 심사 시 고려사항	13
4. 관계 기관 의견	17

I. 제안경위

1. 발 의 자 : 유상범의원 등 12인
2. 발의연월일 : 2024. 6. 19.
3. 회부연월일 : 2024. 6. 20.

II. 제안이유 및 주요내용

1. 제안이유 및 주요내용

최근 북한의 법원 전산망 해킹으로 수년간 대량의 자료가 유출된 사실이 드러난 가운데 현행법상 해킹, 디도스 등 사이버 공격에 대비하기 위해 국가 정보시스템을 체계적으로 점검·관리할 수 있는 근거 조항은 여전히 부재한 실정임.

또한 대부분의 국가기관은 국가정보원을 중심으로 사이버안보 분야가 총괄 관리되고 있는 반면 법원, 헌법재판소, 중앙선거관리위원회 등은 여전히 해당 기관이 자체적으로 관리하고 있어 점차 고도화되는 사이버 위협에 적시 대처하는 데 한계가 있다는 지적이 존재함.

이에 따라 정보통신망 등의 보완조치 및 이행 여부를 점검하는 데 있어 예외 조문을 삭제하는 한편, 국가 정보시스템 안정성 전반에 대해 범정부 차원의 현황조사 및 점검 조항을 신설함으로써 보다 높은

전문성과 체계적인 기관 간 정보 공유·협업을 통해 사이버 위협에 효과적으로 대응하는 제도를 마련하고자 함(안 제56조 및 제56조의2).

2. 참고사항

이 법률안은 유상범의원이 대표발의한 「국가정보원법 일부개정법률안」(의안번호 제672호)의 의결을 전제로 하는 것이므로 같은 법률안이 의결되지 아니하거나 수정의결되는 경우에는 이에 맞추어 조정되어야 할 것임.

Ⅲ. 검토의견

개정안들은 헌법기관을 포함한 국가기관의 사이버안보 및 정보시스템 등의 장애예방·대응 체계를 강화하려는 것임(안 제56조제4항 삭제 및 제56조의2제2항~제6항 신설 등).

현행	유상범의원안
제56조(정보통신망 등의 보안대책 수립·시행) ① 국회, 법원, 헌법재판소, 중앙선거관리위원회 및 행정부는 전자정부의 구현에 필요한 정보통신망과 행정정보 등의 안전성 및 신뢰성 확보를 위한 보안대책을 마련하여야 한다. ② 행정기관의 장은 제1항의 보안대책에 따라 소관 정보통신망 및 행정정보 등의 보안대책을 수립·시행하여야 한다. ③ 행정기관의 장은 정보통신망을 이용하여 전자문서를 보관·유통할 때 위조·변조·훼손 또는 유출을 방지하기 위하여 국가정보원장이 안전성을 확인한 보안조치를 하여야 하고, 국가정보원장은 그 이행 여부를 확인할 수 있다. ④ 제3항을 적용할 때에는 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관	제56조(정보통신망 등의 보안대책 수립·시행) ①~③ (현행과 같음) <u><삭 제></u>

현행	유상범의원안
의 경우에는 해당 기관의 장이 필요하다고 인정하는 경우에만 적용한다. 다만, 필요하지 아니하다고 인정하는 경우에는 해당 기관의 장은 제3항에 준하는 보안조치를 마련하여야 한다. 제56조의2(정보시스템 장애 예방·대응 등) ① <u>행정기관의 장은 해당 기관 및 그 소속 기관의 정보시스템을 안정적으로 운영·관리하기 위하여 정보시스템의 장애 예방 및 대응을 위한 방안을 마련하여야 한다.</u> <u><신 설></u> <u><신 설></u>	제56조의2(정보시스템 장애 예방·대응 등) ① <u>행정기관등과 국회·법원·헌법재판소·중앙선거관리위원회-----정보시스템 및 정보시스템 운영에 필요한 시설을-----</u> <u>-----.</u> ② <u>행정안전부장관은 행정기관등과 국회·법원·헌법재판소·중앙선거관리위원회가 운영·관리하는 정보시스템 및 관련 시설의 안정성을 강화하고 장애를 예방하기 위해 관계기관에게 행정적·재정적·기술적 지원을 받을 수 있다.</u> ③ <u>행정안전부장관은 행정기관등과 국회·법원·헌법재판소·중앙선거관리위원회가 운영·관리하는 정보시스템 및 관련 시설의 안정성을 확인하고 장애를 예방하는데 필요한 현황조사 및 점검을 할 수 있다.</u>

현 행	유상범의원안
<u><신 설></u>	④ 행정안전부장관은 제3항의 현황조사 및 점검 결과에 따라 개선이 필요한 사항에 대해서는 관계기관의 장에게 개선을 권고할 수 있다. 이 경우 해당 관계기관의 장은 개선 필요 사항에 대한 조치계획을 행정안전부장관에게 통보하여야 한다.
<u><신 설></u>	⑤ 행정기관등과 국회·법원·헌법재판소·중앙선거관리위원회의 장은 소관 정보시스템 및 관련 시설에 장애가 발생한 경우 신속하게 행정안전부장관에게 알려야 한다.
<u><신 설></u>	⑥ 행정안전부 장관은 행정기관등과 국회·법원·헌법재판소·중앙선거관리위원회가 운영·관리하는 정보시스템 및 관련 시설에 장애가 발생한 경우 발생 원인을 확인하고 확산 및 재발을 방지하기 위한 조사를 할 수 있다. 이 경우 관계기관의 장은 특별한 사유가 없으면 조사에 적극 협조하여야 한다.
② 제1항에 따른 정보시스템의 장애 예방 및 대응에 필요한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회규칙 및 대통령령으로 정한다.	⑦ 그 밖에 ----- ----- ----- ----- -----.

현행	유상범의원안
	부칙 이 법은 공포한 날부터 시행한다.

1. 헌법기관을 포함한 국가기관의 사이버안보 체계 강화

(안 제56조제4항 삭제)

「전자정부법」 제56조제3항은 행정기관의 장으로 하여금 정보통신망을 이용한 전자문서의 보관·유통 시 위조·변조·훼손 또는 유출 방지를 위하여 국가정보원장이 안전성을 확인한 보안조치를 하도록 하고, 국가정보원장이 그 이행 여부를 확인할 수 있도록 하고 있음¹⁾²⁾.

또한 「전자정부법 시행령」 제69조 및 제70조³⁾는 보안조치와 관련

- 1) 「전자정부법」 제56조(정보통신망 등의 보안대책 수립·시행) ①·② (생략)
- ③ 행정기관의 장은 정보통신망을 이용하여 전자문서를 보관·유통할 때 위조·변조·훼손 또는 유출을 방지하기 위하여 국가정보원장이 안전성을 확인한 보안조치를 하여야 하고, 국가정보원장은 그 이행 여부를 확인할 수 있다.
- ④ (생략)
- 2) 「전자정부법」 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.
 1. (생략)
 2. “**행정기관**”이란 국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다. 이하 같다) 및 그 소속 기관, 지방자치단체를 말한다.
 - 3.~6. (생략)
 7. “**전자문서**”란 컴퓨터 등 정보처리능력을 지닌 장치에 의하여 전자적인 형태로 작성되어 송수신되거나 저장되는 표준화된 정보를 말한다.
 - 8.~9. (생략)
 10. “**정보통신망**”이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말한다.
 - 11.~15. (생략)
- 3) 「전자정부법 시행령」 제69조(전자문서의 보관·유통 관련 보안조치) ① 행정기관의 장은 정보통신망을 이용하여 전자문서를 보관·유통할 때에는 법 제56조제3항에 따라 국가정보원장이 안전성을 확인한 다음 각 호의 보안조치를 하여야 한다.

해서는 국가정보원장이 개발하거나 안전성을 검증한 암호장치와 정보 보호시스템의 도입·운용, 전자문서가 보관·유통되는 정보통신망에 대한 보안대책의 시행, 보안조치 이행 시 국가정보원장에게 보안성 검토 요청을, 보안조치 이행 여부 확인과 관련해서는 점검항목·절차·시기 등의 행정기관의 장에 대한 사전 통보, 이행 여부의 확인 결과 신속한 시정 필요 사항에 대한 조치 요청을 규정하고, 그 밖에 보안조치 및 이행 여부 확인에 필요한 사항은 국가정보원장이 따로 지침으로 정할 수 있도록 하고 있음.

이에 따라 국가정보원장은 「국가정보보안기본지침」 4)5)을 제정하여

1. 국가정보원장이 개발하거나 안전성을 검증한 암호장치와 정보보호시스템의 도입·운용
2. 전자문서가 보관·유통되는 정보통신망에 대한 보안대책의 시행
- ② 행정기관의 장이 제1항의 보안조치를 이행하는 경우에는 미리 국가정보원장에게 보안성 검토를 요청하여야 한다.
- ③ 제1항 및 제2항에서 규정한 사항 외에 정보통신망을 이용한 전자문서의 보관·유통 관련 보안조치에 관하여 필요한 사항은 국가정보원장이 따로 지침으로 정할 수 있다.
- 제70조(보안조치 이행 여부의 확인) ① 국가정보원장은 법 제56조제3항에 따라 정보통신망을 이용한 전자문서의 보관·유통 관련 보안조치의 이행 여부를 확인하는 경우 점검항목·절차·시기 등에 관하여 해당 행정기관의 장에게 미리 통보하여야 한다.
- ② 국가정보원장은 이행 여부의 확인 결과 신속한 시정이 필요하다고 판단하는 경우에는 행정기관의 장에게 필요한 조치를 요청할 수 있다. 이 경우 요청을 받은 행정기관의 장은 특별한 사유가 없으면 이에 따라야 한다.
- ③ 제1항 및 제2항에서 규정한 사항 외에 정보통신망을 이용한 전자문서의 보관·유통 관련 보안조치의 이행 여부 확인에 필요한 사항은 국가정보원장이 따로 지침으로 정할 수 있다.
- 4) 「국가정보보안기본지침」(국가정보원지침) 제1조(목적) 이 지침은 다음 각 호의 법령에 따라 국가정보원장이 정하는 각급기관 정보보안 기본업무를 규정함을 목적으로 한다.
 1. 「국가정보원법」 제4조제1항제1호마목 및 같은 항 제4호 직무에 관련된 정보 및 보안업무의 기획·조정
 2. 「사이버안보 업무규정」 제8조에 따른 사이버안보 기본대책의 수립·시행
(대통령령, 「국가정보원법」에 근거)
 3. 「정보 및 보안업무 기획·조정규정」 제4조제6호에 따라 수립하는 기본지침중에서 정보보안에 관한 사항
(대통령령, 「국가정보원법」에 근거)
 4. 「보안업무규정」 제3조의2에 따라 수립하는 기본정책중에서 정보보안에 관한 사항
(대통령령, 「국가정보원법」에 근거)
 5. 「전자정부법」 제56조제3항에 따른 「전자정부법 시행령」 제69조제3항 및 같은 영 제70조제3항에 따른 지침의 작성
 6. 「정보통신기반보호법」 제6조제4항에 따른 공공분야 보호대책·보호계획 수립지침의 작성
 7. 「공공기록물 관리에 관한 법률 시행령」 제5조에 따른 보안조치
 8. 「국가사이버안전관리규정」 제9조제2항에 따른 지침의 작성
(대통령훈령)
- 5) 「국가정보보안기본지침」은 「전자정부법」 외에 「국가정보원법」, 「정보통신기반보호법」 등에도 근

시행하고 있는데, 동 지침은 정보화사업, 정보통신망 및 정보시스템 등의 보안과 관련한 사항들을 규정⁶⁾하고 있으며, 각 행정기관에서는 동 지침의 내용을 기본으로 하여 해당 기관의 정보보안지침을 마련하여 시행하고 있음⁷⁾⁸⁾.

거를 두고 있음.

6) 「국가정보보안기본지침」(국가정보원지침) 구성 체계

제1장 총칙	목적, 정의, 적용범위 등 규정
제2장 정보화사업 보안	제1절 사업계획 / 제2절 보안성 검토 / 제3절 제품도입 / 제4절 계약 및 사업 수행 / 제5절 보안적합성 검증
제3장 정보통신망 및 정보시스템 보안	제1절 정보통신망 보안 / 제2절 정보시스템 보안 / 제3절 자료 보안 / 제4절 사용자 보안 / 제5절 주요정보통신기반시설 보호
제4장 융합 보안	제1절 정보통신시설 및 기기 보호 / 제2절 전자파 보안
제5장 훈련 및 평가	제1절 훈련 및 진단 / 제2절 정보보안 관리실태 평가
제6장 암호자재 및 암호알고리즘	제1절 기본사항 / 제2절 개발 및 제작 / 제3절 지원요청 및 사용승인 / 제4절 운용 및 관리 / 제5절 정비 및 파기 / 제6절 암호알고리즘
제7장 사이버위협 탐지 및 대응	제1절 보안관제 / 제2절 사고대응
제8장 정보 협력	정보협조 요청, 기관 간 정보공유 협력 등 규정
제9장 보칙	협의회 등, 각급기관 이외 단체에 대한 관리·감독 등 규정

7) 「전자정부법」 제56조(정보통신망 등의 보안대책 수립·시행) ① 국회, 법원, 헌법재판소, 중앙선거관리위원회 및 행정부는 전자정부의 구현에 필요한 정보통신망과 행정정보 등의 안전성 및 신뢰성 확보를 위한 보안대책을 마련하여야 한다.

② 행정기관의 장은 제1항의 보안대책에 따라 소관 정보통신망 및 행정정보 등의 보안대책을 수립·시행하여야 한다.

③·④ (생략)

「사이버안보 업무규정」(대통령령) 제3조의2(사이버안보 업무의 기획·조정) ① 국가정보원장은 제3조 제1호에 따른 사이버안보정보 업무(이하 “사이버안보정보 업무”라 한다) 및 같은 조 제2호에 따른 사이버보안 업무(이하 “사이버보안 업무”라 한다)에 관한 정책의 수립 등 기획업무를 수행하고, 사이버안보정보 업무 및 사이버보안 업무를 효율적·체계적으로 수행하기 위하여 다음 각 호의 지침 등을 수립·시행해야 한다.

1. 사이버안보정보 업무에 관한 기본지침

2. 사이버보안 업무에 관한 기본지침

3. 새로운 유형의 사이버공격·위협에 대응하기 위한 수시 보안대책

② 국가정보원장은 사이버안보정보 업무 및 사이버보안 업무에 대한 조정이 필요한 경우 국가안보에 중대한 영향을 미치는 긴급사안에 대해서는 직접 조정하고, 그 밖의 사안에 대해서는 제1항제1호 및 제2호에 따른 기본지침으로 정하는 바에 따라 조정한다.

제8조(사이버보안 세부지침의 수립·시행) 중앙행정기관등의 장은 제3조의2제1항제2호에 따른 기본지침에 따라 해당 기관의 특성 및 보안수준 등을 반영하여 해당 기관을 대상으로 한 사이버보안 세부지침을 수립·시행해야 한다.

「국가사이버안전관리규정」 제9조(사이버안전대책의 수립·시행 등) ① 중앙행정기관의 장은 소관 정보통신망을 보호하기 위하여 사이버안전대책을 수립·시행하고, 이를 지도·감독하여야 한다.

②~④ (생략)

「국가정보보안기본지침」(국가정보원지침) 제7조(정보보안내규) ① 각급기관의 장은 해당 기관 및 관할 하급기관의 정보보안업무를 규정한 정보보안내규(또는 지침·시행세칙 등)를 이 지침에 저촉되지 아니하는 범위 내에서 수립·시행하여야 한다. 다만, 다른 기관의 행정규칙을 적용하는 경우 별도로 수립하지 아니할 수 있다.

②·③ (생략)

8) 예를 들어 행정안전부는 「행정안전부 정보보안지침」(행정안전부 훈령)을 마련하여 시행하고 있음.

「전자정부법」의 정의 규정에 따르면 동법 제56조제3항의 적용 대상인 ‘행정기관’에는 국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관(이하 “헌법기관”이라 함)이 포함⁹⁾되나, 동법 제56조제4항은 제3항을 적용할 때 헌법기관의 경우에는 해당 기관의 장이 필요하다고 인정하는 경우에만 적용하도록 하고 있음¹⁰⁾.

개정안은 제4항을 삭제하여, 헌법기관에 대해서도 해당 기관의 필요성 인정 여부와 관계 없이 국가정보원장이 안전성을 확인한 보안조치를 하도록 하고, 국가정보원장이 그 이행 여부를 확인할 수 있도록 하려는 것으로, 국가기관에 대한 해킹 위협이 매년 증가하고 있고, 최근에는 2021년 1월 7일 이전부터 2023년 2월 9일까지 법원 전산망에 대한 해킹으로 1,014GB의 자료가 유출된 사실이 국가정보원·검찰청·경찰청의 조사 및 수사 결과 밝혀지기도 한 점¹¹⁾ 등을 고려하면, 헌법기관을 포함한

9) 「전자정부법」 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. (생략)

2. “**행정기관**”이란 국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다. 이하 같다) 및 그 소속 기관, 지방자치단체를 말한다.

3.~15. (생략)

10) 「전자정부법」 제56조(정보통신망 등의 보안대책 수립·시행) ①·② (생략)

③ 행정기관의 장은 정보통신망을 이용하여 전자문서를 보관·유통할 때 위조·변조·훼손 또는 유출을 방지하기 위하여 국가정보원장이 안전성을 확인한 보안조치를 하여야 하고, 국가정보원장은 그 이행 여부를 확인할 수 있다.

④ **제3항을 적용할 때에는 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관의 경우에는 해당 기관의 장이 필요하다고 인정하는 경우에만 적용한다.** 다만, 필요하지 아니하다고 인정하는 경우에는 해당 기관의 장은 제3항에 준하는 보안조치를 마련하여야 한다.

11) 법원은 2024년 3월 4일, “2023년 2월 사법부 전산망에 대한 외부의 침해 시도가 확인되어 자체적인 사안의 조사와 함께 추가적인 피해를 막기 위해 보안조치를 취하였으나, 오랜 조사에도 불구하고 기술적 한계로 인하여 사건의 전모를 파악하기 어려웠고, 2023년 12월 18일부터 외부 보안 전문기관과 함께 심층조사를 진행하였음”을 밝히고, 국민들에게 심려와 불편을 끼친 데 대하여 사과문을 게재하였음.

(“사법부 전산망 침해사고에 대하여 국민들에게 드리는 말씀”, 2024.3.4. 대한민국 법원 홈페이지 참고)

또한, 2024년 5월 11일에는, “수사기관이 5월 8일자로 통보한 침해사고의 수사결과에 따르면, 사법부 전산망 내부 서버에 북한 해킹조직의 소행으로 추정되는 악성코드 침입이 있었고, 1,014GB의 법원 자료가 외부로 전송된 사실이 확인되었음”을 밝히고, “유출된 개인정보를 이용한 2차 피해 방지를 위하여 각별한

국가기관에 대하여 범국가적인 사이버안보체계를 구축하려는 개정안의 입법취지는 타당한 것으로 보임.

2. 헌법기관을 포함한 국가기관의 정보시스템 등의 장애예방·대응 체계 강화(안 제56조의2제1항, 제2항~제6항 신설 등)

「전자정부법」 제56조의2는 행정기관의 장애에 해당 기관 및 그 소속 기관의 정보시스템을 안정적으로 운영·관리하기 위하여 정보시스템의 장애 예방 및 대응을 위한 방안(이하 “장애예방대응방안”이라 함)을 마련하도록 하고, 장애 예방 및 대응에 필요한 사항은 하위 법령으로 정하도록 위임하고 있음¹²⁾.

개정안은 제56조의2를 개정하여 헌법기관을 포함한 국가기관의 정보시스템 장애 예방 및 대응 체계를 보다 강화하려는 것임.

개정안의 주요 내용을 살펴보면, 먼저 장애예방대응방안을 마련해야

주의를 기울여 주실 것”을 추가로 안내하였음.

(“사법부 전산망 침해에 의한 개인정보 유출 추가 안내”, 2024.5.11. 대한민국 법원 홈페이지 참고)

경찰청(국가수사본부)은 2024년 5월 13일, “국가정보원, 검찰청과 합동으로 조사 및 수사를 실시하였으며, 수사 결과 법원 전산망에 대한 침입은 2021. 1. 7. 이전부터 2023. 2. 9.까지 있었고, 이 기간에 1,014GB의 법원 자료가 법원 전산망 외부로 전송되었으며, 그 중 회생 사건 관련 파일 5,171개(4.7GB)를 법원 전산망 외부에서 발견하여 유출이 사실임을 확인하였음”과 “범행에 사용된 악성 프로그램, 서버 결제내역(가상자산), 아이피 주소 등을 기존 북한발로 규명된 해킹 사건과 종합적으로 비교·분석한 결과, 본 사건을 북한 해킹조직의 소행으로 판단하였음”을 발표하였음.

(“북, 법원 전산망 해킹 및 자료 1,014GB 절취 - 개인회생에 관한 문서 파일 5,171개(4.7GB) 유출 확인”, 2024.5.13. 경찰청 보도자료 참고)

12) 「전자정부법」 제56조의2(정보시스템 장애 예방·대응 등) ① 행정기관의 장은 해당 기관 및 그 소속 기관의 정보시스템을 안정적으로 운영·관리하기 위하여 정보시스템의 장애 예방 및 대응을 위한 방안을 마련하여야 한다.

② 제1항에 따른 정보시스템의 장애 예방 및 대응에 필요한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회규칙 및 대통령령으로 정한다.

하는 주체에 헌법기관을 명시하고, 장애예방대응방안 마련 대상에 정보시스템 운영시설을 추가하여(이상 안 제1항) 장애 예방 및 대응의 범위를 보다 확대하고 있음.

또한 행정기관등과 헌법기관의 정보시스템 및 관련 시설에 대하여 ‘행정안전부장관의 현황조사 및 점검 → 개선권고 → 개선 조치계획 통보’로 이어지는 안정성 강화 및 장애 예방 방안(안 제3항 및 제4항)과 장애발생 시 ‘행정안전부장관에게 신속 통보 → 행정안전부장관의 장애 원인 조사 및 관계기관의 장의 적극 협조’라는 장애 대응 및 재발 방지 방안(안 제5항 및 제6항)을 규정하고 있음.

[개정안에 따른 정보시스템 및 운영시설 장애예방·대응 체계 강화 방안]

구 분	현 행	개 정 안
-안 제1항- 장애 예방 및 대응 방안 마련 주체에 헌법기관 명시	행정기관등의 장	행정기관등의 장 + <u>국회·법원·헌법재판소·중앙선거 관리위원회</u> 의 장
-안 제1항- 장애 예방 및 대응 방안 마련 대상에 정보시스템 운영 시설 추가	정보시스템의 안정적 운영·관리	정보시스템의 안정적 운영·관리 + <u>정보시스템 운영 시설</u> 의 안정적 운영·관리
-안 제2항- 행안부장관에 대한 행정적·재정적·기술적 지원	<신 설>	행정안전부장관: 행정기관등과 국 회·법원·헌법재판소·중앙선거관리 위원회가 운영·관리하는 정보시스 템 및 관련 시설의 안정성을 강화 하고 장애를 예방하기 위해 <u>관계 기관에게 행정적·재정적·기술적 지원을 받을 수 있음.</u>
-안 제3항- 행안부장관의	<신 설>	행정안전부장관: 행정기관등과 국

구 분	현 행	개 정 안
현황조사 및 점검		회·법원·헌법재판소·중앙선거관리위원회가 운영·관리하는 정보시스템 및 관련 시설의 <u>안전성 확인</u> 과 <u>장애 예방</u> 에 필요한 <u>현황조사 및 점검</u> 을 할 수 있음.
-안 제4항- 행안부장관의 개선 권고	<신 설>	행정안전부장관: 현황조사 및 점검 결과 개선 필요 사항에 대해 <u>관계기관의 장에게 개선을 권고</u> 할 수 있음.
-안 제4항- 행안부장관에 대한 개선 조치계획 통보	<신 설>	관계기관의 장: 개선 필요 사항에 대한 <u>조치계획</u> 을 <u>행정안전부장관에게 통보</u> 해야 함.
-안 제5항- 장애 발생 시 행안부장관에 대한 신속 통보	<신 설>	행정기관등과 국회·법원·헌법재판소·중앙선거관리위원회의 장: 소관 정보시스템 및 관련 시설에 <u>장애 발생</u> 시 <u>신속하게 행정안전부장관에게 알려야 함</u> .
-안 제6항- 행안부장관의 장애 원인 조사	<신 설>	행정안전부장관: 행정기관등과 국회·법원·헌법재판소·중앙선거관리위원회가 운영·관리하는 정보시스템 및 관련 시설에 장애가 발생한 경우 <u>발생 원인을 확인</u> 하고 <u>확산 및 재발을 방지</u> 하기 위한 <u>조사</u> 를 할 수 있음.
-안 제6항- 행안부장관의 장애 원인 조사에 대한 적극 협조	<신 설>	관계기관의 장: 특별한 사유가 없으면 <u>조사에 적극 협조</u> 해야 함.

정보시스템 운영시설의 안전성 강화와 관련해서는 2022.10.15. SK C&C 판교 데이터센터 화재로 입주기업인 카카오 및 네이버의 서비스에

장시간 장애가 발생하였고, 장애복구 및 기능 정상화에 카카오는 약 127시간, 네이버는 약 20분~12시간이 소요¹³⁾되어 많은 국민들이 불편을 겪으면서 제도개선 필요성이 제기된 바 있음.

또한 2023년 11월과 12월에는 지방행정전산서비스 장애로 지방자치단체 민원실과 정부24 등의 대민서비스가 중단되고, 나라장터 홈페이지 접속에 문제가 생기는 등 디지털 행정서비스의 불안정성과 대응 과정의 문제점이 노출되기도 하였는바¹⁴⁾, 국가기관의 정보시스템 및 운영시설에 대하여 범국가적인 장애 예방·대응체계를 구축하려는 개정안의 입법취지는 타당한 것으로 보임.

3. 개정안 심사 시 고려사항

동 개정안의 심사에 있어서는 다음 사항들을 고려할 필요가 있어 보임.

개정안과 유사한 내용을 규정하고 있는 법률로는 해킹, 컴퓨터바이러스 등을 이용한 전자적 침해행위 대비를 목적으로 하는 「정보통신기반 보호법」¹⁵⁾이 있음. 동법은 국무총리 소속 정보통신기반위원회¹⁶⁾

13) 과학기술정보통신부 보도자료, 2022.12.6. “디지털서비스 장애 조사결과 발표, 시정요구 - 에스케이 씨앤시, 카카오, 네이버, 이행결과 및 향후 계획 1개월 내에 제출토록” 참고

14) “디지털서비스 국민신뢰 제고 대책”, 관계부처 합동 2024.1.31. 참고

15) 「**정보통신 기반보호법**」 제1조(목적) 이 법은 **전자적 침해행위에 대비**하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하는 것을 목적으로 한다.

제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

1. “**정보통신기반시설**”이라 함은 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호에 따른 정보통신망을 말한다.
2. “**전자적 침해행위**”란 다음 각 목의 방법으로 정보통신기반시설을 공격하는 행위를 말한다.

에서 헌법기관을 포함한 국가기관의 주요정보통신기반시설보호계획 등을 심의¹⁷⁾하고, 동 위원회의 실무위원회에 헌법기관의 공무원이 위원으로 참여¹⁸⁾할 수 있으며, 국가정보원장이 주요정보통신기반시설보호

가. 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등의 방법
나. 정상적인 보호·인증 절차를 우회하여 정보통신기반시설에 접근할 수 있도록 하는 프로그램이나 기술적 장치 등을 정보통신기반시설에 설치하는 방법

3. “침해사고”란 전자적 침해행위로 인하여 발생한 사태를 말한다.

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조(정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. “정보통신망”이란 「전기통신사업법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신 체제를 말한다.

2.~13. (생략)

16) 「정보통신 기반보호법」 제3조(정보통신기반보호위원회) ① 제8조에 따라 지정된 주요정보통신기반시설(이하 “주요정보통신기반시설”이라 한다)의 보호에 관한 사항을 심의하기 위하여 국무총리 소속하에 정보통신기반보호위원회(이하 “위원회”라 한다)를 둔다.

② 위원회의 위원은 위원장 1인을 포함한 25인 이내의 위원으로 구성한다.

③ 위원회의 위원장은 국무조정실장이 되고, 위원회의 위원은 대통령령으로 정하는 중앙행정기관의 차관급 공무원과 위원장이 위촉하는 사람으로 한다.

④ 위원회의 효율적인 운영을 위하여 위원회에 공공분야와 민간분야를 각각 담당하는 실무위원회를 둔다.

⑤ 위원회 및 실무위원회의 구성·운영 등에 관하여 필요한 사항은 대통령령으로 정한다.

17) 「정보통신 기반보호법」 제4조(위원회의 기능) 위원회는 다음 각호의 사항을 심의한다.

1. 주요정보통신기반시설 보호정책의 조정에 관한 사항

2. 제6조제1항에 따른 주요정보통신기반시설에 관한 보호계획의 종합·조정에 관한 사항

3. 제6조제1항에 따른 주요정보통신기반시설에 관한 보호계획의 추진 실적에 관한 사항

4. 주요정보통신기반시설 보호와 관련된 제도의 개선에 관한 사항

4의2. 제8조제5항에 따른 주요정보통신기반시설의 지정 및 지정 취소에 관한 사항

4의3. 제8조의2제1항 후단에 따른 주요정보통신기반시설의 지정 여부에 관한 사항

5. 그 밖에 주요정보통신기반시설 보호와 관련된 주요 정책사항으로서 위원장이 회의에 부치는 사항

18) 「정보통신 기반보호법 시행령」 제5조(실무위원회의 구성·운영) ① 법 제3조제4항에 따라 위원회에 두는 공공분야를 담당하는 실무위원회(이하 “공공분야 실무위원회”라 한다)와 민간분야를 담당하는 실무위원회(이하 “민간분야 실무위원회”라 한다)는 각각 위원장 1명을 포함한 25명 이내의 위원으로 구성한다.

② 공공분야 실무위원회의 위원장은 국가정보원 차장이 되고, 민간분야 실무위원회의 위원장은 과학기술정보통신부 제2차관이 되며, 각 실무위원회 위원장은 해당 실무위원회의 회의를 소집하고 그 의장이 된다.

③ 각 실무위원회의 위원은 다음 각 호의 어느 하나에 해당하는 사람 중에서 각 실무위원회의 위원장이 임명하거나 위촉한다.

1. 법 제8조에 따라 지정된 주요정보통신기반시설(이하 “주요정보통신기반시설”이라 한다)을 관할하는 중앙행정기관(이하 “관계중앙행정기관”이라 한다)의 고위공무원단에 속하는 공무원 또는 그에 상당하는 공무원

2. 주요정보통신기반시설을 관리하는 기관(이하 “관리기관”이라 한다)의 임원 또는 직원

④ 각 실무위원회는 다음 각 호의 구분에 따른 주요정보통신기반시설의 보호에 관하여 위원회의 심의를 지원한다.

1. 공공분야 실무위원회: 다음 각 목의 주요정보통신기반시설

가. 중앙행정기관·지방자치단체 및 그 소속 기관의 장이 관리하는 주요정보통신기반시설

나. 국회·법원·헌법재판소·중앙선거관리위원회 및 그 소속 기관의 장이 관리하는 주요정보통신기반시설

다. 「전자정부법」 제2조제3호에 따른 공공기관이 관리하는 주요정보통신기반시설

2. 민간분야 실무위원회: 제1호에 따른 주요정보통신기반시설 외의 주요정보통신기반시설

⑤ 각 실무위원회는 제4항 각 호의 구분에 따른 주요정보통신기반시설의 보호에 관하여 위원회가 위임하거나 위원회의 위원장이 지시한 사항을 검토·심의한다.

⑥ (생략)

대책의 이행 여부를 확인¹⁹⁾할 수 있는 체계를 규정하고 있음.

「정보통신기반 보호법」이 전자적 침해행위에 대하여 헌법기관을 포함한 국가적인 대응체계를 규정하고 있는 것은 전자적 방식의 기술이 발달하면서 이를 이용한 위협에 대해 각 기관이 가진 전문적 지식과 기술을 공동 활용하여 대처할 필요성이 커졌기 때문인 것으로 보이며, 개정안 또한 이같은 이유로 「전자정부법」 개정을 통해 범국가적인 사이버안보체계를 구축하려는 취지로 보임.

다만, 「전자정부법」은 각 헌법기관을 중앙행정기관 및 지방자치단체와 분리하여 각각 독립적이고 자율적으로 전자정부를 구현하도록 규정²⁰⁾

19) 「정보통신 기반보호법」 제5조의2(주요정보통신기반시설보호대책 이행 여부의 확인) ① 과학기술정보통신부장관과 국가정보원장 등 대통령령으로 정하는 국가기관의 장(이하 “국가정보원장등”이라 한다)은 관리기관에 대하여 주요정보통신기반시설보호대책의 이행 여부를 확인할 수 있다.

② 과학기술정보통신부장관과 국가정보원장등은 제1항에 따른 확인을 위하여 필요한 경우 관계중앙행정기관의 장에게 제5조제2항에 따라 제출받은 주요정보통신기반시설보호대책 등의 자료 제출을 요청할 수 있다.

③ 과학기술정보통신부장관과 국가정보원장등은 제1항에 따라 확인한 주요정보통신기반시설보호대책의 이행 여부를 관계중앙행정기관의 장에게 통보할 수 있다.

④ 제1항에 따른 주요정보통신기반시설보호대책 이행 여부의 확인절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

「정보통신 기반보호법 시행령」 제9조의2(주요정보통신기반시설보호대책 이행 여부의 확인) ① (생략)

② 법 제5조의2제1항에 따라 과학기술정보통신부장관, 국가정보원장 및 국방부장관은 다음 각 호의 구분에 따른 관할 주요정보통신기반시설에 대한 관리기관의 주요정보통신기반시설보호대책 이행 여부를 확인할 수 있다.

1. 과학기술정보통신부장관: 제5조제4항제2호에 따른 주요정보통신기반시설

2. 국가정보원장: 제5조제4항제1호에 따른 주요정보통신기반시설(제3호의 국방 분야 주요정보통신기반시설은 제외한다)

3. 국방부장관: 국방 분야 주요정보통신기반시설

③ 과학기술정보통신부장관, 국가정보원장 및 국방부장관은 법 제5조의2에 따라 주요정보통신기반시설보호대책 이행 여부를 확인하기 위하여 필요한 자료의 제출을 제2항의 구분에 따른 관할 주요정보통신기반시설 관리기관에 요청하고, 해당 주요정보통신기반시설보호대책에 따른 보호조치의 세부적인 내용을 확인·점검할 수 있다.

④ 과학기술정보통신부장관과 국가정보원장은 법 제5조의2에 따라 주요정보통신기반시설보호대책의 이행 여부를 확인하려는 경우 미리 확인 절차 등에 관하여 관계중앙행정기관의 장과 협의하여야 하고, 과학기술정보통신부장관, 국가정보원장 및 국방부장관은 확인 절차 등에 관하여 해당 관리기관에 통보하여야 한다.

⑤·⑥ (생략)

20) 「전자정부법」 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1.~3. (생략)

하고 있고, 다른 법률의 경우에도 헌법기관의 독립성을 존중하는 취지로 헌법기관을 행정부의 권한 행사 범위에서 제외²¹⁾하거나 헌법기관에서 자체적인 지침을 정하여 시행²²⁾할 수 있도록 하고 있는 사례들이 있는바, 헌법기관들은 개정안에 대하여 헌법상 권력분립의 원칙에 따른 헌법기관의 독립성과 자율성이 침해될 수 있다는 의견들을 제시하고 있음.

4. “중앙사무관장기관”이란 국회 소속 기관에 대하여는 국회사무처, 법원 소속 기관에 대하여는 법원행정처, 헌법재판소 소속 기관에 대하여는 헌법재판소사무처, 중앙선거관리위원회 소속 기관에 대하여는 중앙선거관리위원회사무처, 중앙행정기관 및 그 소속 기관과 지방자치단체에 대하여는 행정안전부를 말한다.

5.~15. (생략)

제5조(전자정부기본계획의 수립) ① 중앙사무관장기관의 장은 전자정부의 구현·운영 및 발전을 위하여 5년마다 제5조의2제1항에 따른 행정기관등의 기관별 계획을 중합하여 전자정부기본계획을 수립하여야 한다.

②·③ (생략)

④ 전자정부기본계획의 수립 절차 등에 관하여 필요한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회규칙 및 대통령령으로 정한다.

제7조(전자정부서비스의 신청 등) ①~⑤ (생략)

⑥ 전자화문서의 활용 및 진본성 확인 등을 위하여 필요한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회규칙 및 대통령령으로 정한다.

제29조(행정전자서명의 인증) ①~④ (생략)

⑤ 행정전자서명의 인증업무에 관하여 필요한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회규칙 및 대통령령으로 정한다.

제32조(전자적 업무수행 등) ①·② (생략)

③ 행정기관등의 장은 필요하면 소속 직원으로 하여금 특정한 근무장소를 정하지 아니하고 정보통신망을 이용한 온라인 원격근무를 하게 할 수 있다. 이 경우 행정기관등의 장은 정보통신망에 대한 불법적인 접근의 방지와 그 밖의 보호대책을 마련하여야 한다.

④ (생략)

⑤ 제1항부터 제4항까지의 전자적 업무수행을 촉진하기 위하여 필요한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회규칙 및 대통령령으로 정한다.

21) 「공공기관의 정보공개에 관한 법률」 제24조(제도 총괄 등) ① (생략)

② 행정안전부장관은 위원회가 정보공개제도의 효율적 운영을 위하여 필요하다고 요청하면 공공기관(국회·법원·헌법재판소 및 중앙선거관리위원회는 제외한다)의 정보공개제도 운영실태를 평가할 수 있다.

③~⑤ (생략)

「공공데이터의 제공 및 이용에 관한 법률」 제9조(공공데이터의 제공 운영실태 평가) ① 행정안전부장관은 매년 공공기관(국회·법원·헌법재판소 및 중앙선거관리위원회는 제외한다, 이하 이 조에서 같다)을 대상으로 공공데이터의 제공기반조성, 제공현황 등 제공 운영실태를 대통령령으로 정하는 바에 따라 평가하여야 한다.

②~④ (생략)

22) 「개인정보 보호법」 제12조(개인정보 보호지침) ① 보호위원회는 개인정보의 처리에 관한 기준, 개인정보 침해의 유형 및 예방조치 등에 관한 표준 개인정보 보호지침(이하 “표준지침”이라 한다)을 정하여 개인정보처리자에게 그 준수를 권장할 수 있다.

② 중앙행정기관의 장은 표준지침에 따라 소관 분야의 개인정보 처리와 관련한 개인정보 보호지침을 정하여 개인정보처리자에게 그 준수를 권장할 수 있다.

③ 국회, 법원, 헌법재판소 및 중앙선거관리위원회는 해당 기관(그 소속 기관을 포함한다)의 개인정보 보호지침을 정하여 시행할 수 있다.

따라서 개정안의 심사에 있어서는 사이버안보 및 정보시스템 등의 장애 예방·대응이라는 전문 분야의 특수성과 헌법상 권력분립의 원리에 따른 헌법기관의 독립성 및 자율성 보장을 함께 고려하여 심사할 필요가 있어 보임.

4. 관계 기관 의견

동 개정안에 대한 관계 기관의 의견은 다음과 같음.

국회사무처는 국회는 권력분립의 원칙에 따라 행정부를 감시·견제하는 헌법상의 역할을 수행하는 기관으로, 이를 위한 국회의원의 의정활동을 지원하는 다수의 정보시스템이 운영되고 있는데, 개정안과 같이 하는 경우 국회 정보시스템의 구축·운영·보안 등에 관하여 대통령 소속인 국가정보원 및 행정안전부의 관리와 통제를 받는 것이 되어, 권력분립의 원칙과 헌법기관의 독립성을 침해할 우려가 있고, 또한 정보시스템 내 민감한 국회의원 의정활동 정보의 보안성이 침해될 가능성이 있다는 입장임.

법원행정처는 사법부의 독립성, 자율성을 침해할 수 있으므로 신중한 접근이 필요하고, 개정안에 따른 국가정보원 및 행정안전부의 수행 기능이 「국가정보원법」 및 「정부조직법」에 따른 직무 수행 범위에 포함되지 않는다는 입장임²³⁾²⁴⁾.

23) 「국가정보원법」 제4조(직무) ① 국정원은 다음 각 호의 직무를 수행한다.

1. 다음 각 목에 해당하는 정보의 수집·작성·배포
가. 국외 및 북한에 관한 정보

헌법재판소사무처는 국가정보원 및 행정안전부가 헌법재판소 정보 시스템 및 운영시설의 안정성 전반에 대한 조사·점검을 할 수 있도록 하는 것은 권력분립의 원칙과 헌법기관의 독립성 존중 차원에서 신중하게 접근할 필요가 있고, 특히, 조사·점검 과정에서 헌법재판소가 국가정보원과 행정안전부의 통제를 받을 여지가 있는바, 헌법재판소 정보 시스템 및 데이터 관리의 자율성이 침해될 우려가 있다는 입장임.

중앙선거관리위원회사무처는 정치권 및 폭넓은 국민의 공감대를 바탕으로 심도있는 논의를 거쳐 입법정책적으로 결정할 사안으로 보인다는

-
- 나. 방첩(산업경제정보 유출, 해외연계 경제질서 교란 및 방위산업침해에 대한 방첩을 포함한다), 대테러, 국제범죄조직에 관한 정보
- 다. 「형법」 중 내란의 죄, 외환의 죄, 「군형법」 중 반란의 죄, 암호 부정사용의 죄, 「군사기밀 보호법」에 규정된 죄에 관한 정보
- 라. 「국가보안법」에 규정된 죄와 관련되고 반국가단체와 연계되거나 연계가 의심되는 안보침해행위에 관한 정보
- 마. 국제 및 국가배후 해킹조직 등 사이버안보 및 위성자산 등 안보 관련 우주 정보
2. 국가 기밀(국가의 안전에 대한 중대한 불이익을 피하기 위하여 한정된 인원만이 알 수 있도록 허용되고 다른 국가 또는 집단에 대하여 비밀로 할 사실·물건 또는 지식으로서 국가 기밀로 분류된 사항만을 말한다. 이하 같다)에 속하는 문서·자재·시설·지역 및 국가안전보장에 한정된 국가 기밀을 취급하는 인원에 대한 보안 업무. 다만, 각급 기관에 대한 보안감사는 제외한다.
3. 제1호 및 제2호의 직무수행에 관련된 조치로서 국가안보와 국익에 반하는 북한, 외국 및 외국인·외국 단체·초국가행위자 또는 이와 연계된 내국인의 활동을 확인·견제·차단하고, 국민의 안전을 보호하기 위하여 취하는 대응조치
4. **다음 각 목의 기관 대상 사이버공격 및 위협에 대한 예방 및 대응**
- 가. 중앙행정기관(대통령 소속기관과 국무총리 소속기관을 포함한다) 및 그 소속기관과 국가인권위원회, 고위공직자범죄수사처 및 「행정기관 소속 위원회의 설치·운영에 관한 법률」에 따른 위원회
- 나. 지방자치단체와 그 소속기관
- 다. 그 밖에 대통령령으로 정하는 공공기관
5. 정보 및 보안 업무의 기획·조정
6. 그 밖에 다른 법률에 따라 국정원의 직무로 규정된 사항
- ② 원장은 제1항의 직무와 관련하여 직무수행의 원칙·범위·절차 등이 규정된 정보활동기본지침을 정하여 국회 정보위원회에 이를 보고하여야 한다. 정보활동기본지침을 개정할 때에도 또한 같다.
- ③ 국회 정보위원회는 정보활동기본지침에 위법하거나 부당한 사항이 있다고 인정되면 재적위원 3분의 2 이상의 찬성으로 시정이나 보완을 요구할 수 있으며, 원장은 특별한 사유가 없으면 그 요구에 따라야 한다.
- ④ 제1항제1호부터 제4호까지의 직무 수행을 위하여 필요한 사항과 같은 항 제5호에 따른 기획·조정의 범위와 대상 기관 및 절차 등에 관한 사항은 대통령령으로 정한다.
- 「정부조직법」 제34조(행정안전부) ① 행정안전부장관은 국무회의의 서무, 법령 및 조약의 공포, 정부조직과 정원, 상훈, 정부혁신, 행정능률, 전자정부, 정부청사의 관리, 지방자치제도, 지방자치단체의 사무지원·재정·세제, 낙후지역 등 지원, 지방자치단체간 분쟁조정, 선거·국민투표의 지원, 안전 및 재난에 관한 정책의 수립·총괄·조정, 비상대비, 민방위 및 방재에 관한 사무를 관장한다.
- ②~⑧ (생략)
- 24) 국가정보원의 직무와 관련해서는, 국가정보원의 사이버공격 및 위협에 대한 예방 및 대응 적용 기관에 헌법기관을 포함하는 내용의 “국가정보원법 일부개정법률안(의안번호 제2200672호, 유상범의원 대표발의)”이 발의되어 정보위원회에 계류되어 있음.

입장임.

행정안전부는 사이버 공격에 대한 국가기관의 정보시스템 안전조치와 장애 예방·대응을 위해 정보시스템 조사·점검, 정보공유 및 원인조사 체계가 필요하다는 입장임.

개정안의 비용추계와 관련해서는 비용추계 미대상사유서가 제출되었음.

문 의 처
02)6788-5339