



제429회 국회(정기회)
제 1 차 정 보 위 원 회

국가정보원법 일부개정법률안

검 토 보 고

〈사이버공격·위협에 대한 예방·대응 대상기관 확대〉

■ 강선영의원 대표발의(의안번호 제2209532호)

2025. 9.

정 보 위 원 회

수석전문위원 김건오

목 차

I. 제안경위	1
II. 제안이유 및 주요내용	1
III. 검토의견	3
※ 참고자료	10

I. 제안경위

1. 발 의 자 : 강선영 · 고동진 · 이인선 · 강대식 · 곽규택 · 김 건
박준태 · 임종득 · 김대식 · 유용원 의원(10인)
2. 발의연월일 : 2025. 4. 1.
3. 회부연월일 : 2025. 4. 2.

II. 제안이유 및 주요내용

「정보통신기반 보호법」에 따르면 중앙선거관리위원회는 주요정보통신기반시설로 지정되어 있기 때문에 현행법상 국가정보원의 보안점검 대상에 포함되어 있지 않음.

그리하여 중앙선거관리위원회는 여러 차례 국가정보원의 요구에도 불구하고 보안점검을 받지 않음. 그 와중에 선거관리위원회는 2023년 감사원 감사에서 채용비리 문제가 발견되었고, 이후 중앙선거관리위원회가 국가정보원의 보안점검을 수용하여 서버 전체 내용의 약 5%에 해당하는 일부에 대해 점검을 실시하였는데, ‘통합선거인 명부 시스템’과 ‘투표분류기’ 해킹 취약, ‘개표시스템’ 보안관리 미흡, 단순한 패스워드 사용으로 인한 손쉬운 시스템 침투 가능, 북한 ‘김수키’ 조직의 악성코드 감염에 따른 업무 자료 유출 사실 확인 등 중앙선거관리위원회 서버의 보안 수준은 100점 만점에 31.5점 수준으로 평가됨.

이에 따라 국민적 의혹이 야기되었고, 급기야 대통령은 ‘중앙선거관

리위원회 서버의 취약성' 문제를 밝히기 위해 비상계엄을 선포하기도 하였으며, 2024년 12월 3일 비상계엄 선포 당일 계엄군이 중앙선거관리위원회에 진입하였을 때에도 신원조사도 받지 않은 용역업체 직원이 서버실을 관리하면서 출입문을 개방해 준 사실이 밝혀지면서 국민들의 의혹은 더욱 증폭되고 있는 실정임.

유권자의 개인정보 보호와 자유민주주의 질서 유지, 국민에게 개인이 행사하는 투표가 선거에 차질 없이 반영된다는 믿음을 주기 위해서는 중앙선거관리위원회의 보안점검이 주기적으로 이루어져야 하며, 그 결과가 국민들에게 객관적이고 투명하게 제공되어야 함.

이에 국가정보원 보안점검 대상에 중앙선거관리위원회를 포함시켜 중앙선거관리위원회에 대한 국민적 의혹을 해소하려는 것임(안 제4조의제1항제4호가목 신설).

Ⅲ. 검토의견

개정안은 국가정보원이 사이버공격 및 위협에 대한 예방 및 대응 직무를 수행할 수 있는 기관에 “중앙선거관리위원회”를 추가하려는 것임.

<신·구조문대비표>

현행	개정안
제4조(직무) ① 국정원은 다음 각 호의 직무를 수행한다. 1. ~ 3. (생략) 4. 다음 각 목의 기관 대상 사이버공격 및 위협에 대한 예방 및 대응 <u><신설></u> 가. ~ 다. (생략) 5.·6. (생략) ② ~ ④ (생략)	제4조(직무) ① ----- -----. 1. ~ 3. (현행과 같음) 4. ----- ----- ----- 가. 중앙선거관리위원회 나. ~ 라. (현행 가목부터 다목까지와 같음) 5.·6. (현행과 같음) ② ~ ④ (현행과 같음)

현행법에 따라 국가정보원은 중앙행정기관·지방자치단체와 그 소속기관, 대통령령으로 정하는 공공기관, 지방공사·지방공단 등¹⁾을 대

1) 「국가정보원법」

제4조(직무) ① 국정원은 다음 각 호의 직무를 수행한다.

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

상으로 사이버공격 및 위협에 대한 예방·대응 업무를 수행 중임.

사이버공격 및 위협에 대한 예방·대응 업무는 정보시스템 및 전산망에 대한 보안관리 수준 측정, 조직·인력·예산·직무교육 등 사이버보안 실태 평가, 사이버공격·위협의 탐지 및 보안관제, 경보 발령, 사고 발생 시 공격주체 규명·원인 분석 및 피해내역 확인 등을 위한 조사 실시 등을 포함하는 것임(<참고> 「사이버안보 업무규정」에 따른 예방·대응 업무 범위 참조).

현재 국회, 법원, 헌법재판소 및 선거관리위원회는 자체 점검 및 보안관제를 실시하고 있음. 국가정보원은 해당 기관의 요청이 있는 경우에만 예방·대응 업무를 지원하고 있으며, 직무 수행 과정에서 위협을 탐지한 경우 해당 기관이 자체 조치할 수 있도록 관련 정보를 제공하고 있음.

「전자정부법」 제56조제3항 및 제4항²⁾에 따라 중앙선거관리위원회

-
- 나. 지방자치단체와 그 소속기관
 - 다. 그 밖에 대통령령으로 정하는 공공기관

「사이버안보 업무규정」(대통령령)

제7조(사이버보안 업무 대상 공공기관의 범위) 법 제4조제1항제4호다목에서 “대통령령으로 정하는 공공기관”이란 다음 각 호의 기관을 말한다.

1. 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관
2. 「지방공기업법」에 따른 지방공사 및 지방공단
- 2의2. 「지방자치단체 출자·출연 기관의 운영에 관한 법률」 제2조제1항에 따른 출자·출연 기관 중 해당 지방자치단체의 조례로 정하는 기관
3. 특별법에 따라 설립된 법인. 다만, 「지방문화원진흥법」에 따른 지방문화원 및 특별법에 따라 설립된 조합·협회는 제외한다.
4. 「초·중등교육법」, 「고등교육법」 및 그 밖의 다른 법률에 따라 설치된 국립·공립 학교
5. 「정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조제1항 및 「과학기술분야 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조제1항에 따른 연구기관

2) 「전자정부법」

제56조(정보통신망 등의 보안대책 수립·시행) ① 국회, 법원, 헌법재판소, 중앙선거관리위원회 및 행정부는 전자정부의 구현에 필요한 정보통신망과 행정정보 등의 안전성 및 신뢰성 확보

등 헌법상 독립기관의 행정사무를 처리하는 기관의 장은 필요하다고 인정하는 경우에는 사이버안보 관련 업무 협조를 국가정보원에 요청할 수 있고, 국가정보원은 이 같은 요청이 있는 경우에만 사이버위협 예방·대응 업무를 지원 중임.

개정안과 관련하여 헌법기관 중 중앙선거관리위원회에 대하여만 국가정보원이 예방·대응 직무를 수행하는 것이 타당한지 여부가 검토될 필요가 있음.

2023년 공공기관을 대상으로 한 국제 해킹조직의 사이버 공격 시도가 하루 평균 162만여 건에 이르는 등³⁾ 국가기관에 대한 해킹 위협이 매년 증가하고 있고, 최근 국가정보원·검찰청·경찰청의 조사 및 수사 결과 2021년 1월 7일 이전부터 2023년 2월 9일까지 법원 전산망에 대한 해킹으로 1,014GB의 자료가 유출된 사실이 밝혀진 바 있음⁴⁾.

를 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 기관의 경우에는 해당 기관의 장이 필요하다고 인정하는 경우에만 적용한다. 다만, 필요하지 아니하다고 인정하는 경우에는 해당 기관의 장은 제3항에 준하는 보안조치를 마련하여야 한다.

3) KBS 뉴스, 「국정원 “공공분야 해킹 80%가 북한발…김정은 진두지휘”」 2024.1.24. 및 허백윤, 「공공기관 하루 162만건 해킹 위협 85% 北中 소행… “선거 공작 우려”」, 서울신문, 2024.1.25.

4) “경찰청(국가수사본부)은 ‘법원 전산망 해킹 및 자료 유출 사건’에 대하여 국가정보원, 검찰청과 합동으로 조사 및 수사를 실시하였다. 수사 결과, 법원 전산망에 대한 침입은 2021. 1. 7. 이전부터 2023. 2. 9.까지 있었다. 이 기간에 1,014GB의 법원 자료가 법원 전산망 외부로 전송되었고, 그중 회생 사건 관련 파일 5,171개(4.7GB)를 법원 전산망 외부에서 발견하여 유출이 사실임을 확인하였다. (중략) 경찰청·국가정보원·검찰청에서는 이번 범행에 사용된 악성 프로그램, 서버 결제내역(가상자산), 아이피 주소 등을 기존 북한발로 규명된 해킹 사건과 종합적으로 비교·분석한 결과, 본 사건을 북한 해킹조직의 소행으로 판단하였다.” (경찰청 보도자료, 「북, 법원 전산망 해킹 및 자료 1,014GB 절취: 개인회생에 관한 문서 파일 5,171개(4.7GB) 유출 확인」, 2024.5.12.)

국가정보원은 2023년 6월 중앙선거관리위원회가 국회 교섭단체 추천 여야 참관인들의 참여 하에 보안점검을 요청함에 따라 같은 해 7월 3일부터 9월 22일까지 선거관리위원회 및 한국인터넷진흥원(KISA)과 합동으로 선거관리위원회 주요 시스템을 대상으로 보안점검을 실시하였고, 그 결과 중앙선거관리위원회는 2023년 11월 ‘정보보안시스템 개선 종합대책’을 발표하였고 이후 발견된 주요 문제점들을 모두 개선하였음⁵⁾.

그 밖에 국가정보원은 최근 10년간 악성코드 감염 및 자료 유출 등 총 14건의 사이버 위협정보(공격 일시·대상 IP 등 포함)를 선거관리위원회에 통보하였다고 함.

개정안은 사이버보안 관련 고도의 전문성을 보유한 국가정보원이 중앙선거관리위원회에 대한 예방 및 대응 직무를 실시할 경우 외부 사이버공격으로부터 국가 정보시스템 및 전산망 보호를 강화할 수 있다는 취지에서 발의된 것으로 이해됨.

다만, 개정안에 대해서는 다음과 같은 국가정보원과 중앙선거관리위원회의 의견 및 현행 법률과의 체계 정합성 등을 고려하여 검토될 필요가 있어 보임.

먼저, 개정안과 관련하여 국가정보원은 「국가정보원법」 개정을 통해 선거관리위원회가 국가정보원의 사이버 위협 예방·대응 대상기관

5) 국가정보원은 선관위 점검 당시 확인된 보안 취약점에 대하여 2024년 1월 및 3월 선거관리위원회와 합동으로 두 차례 점검하여 대부분 조치된 것을 확인하였다는 설명임.

에 포함될 경우 보안체계가 강화될 것으로 기대된다는 의견을 제시하면서, 한편으로는 선거관리위원회의 동의가 전제되어야 할 것이라는 의견을 제시하고 있음⁶⁾.

그런데 개정안에 대해서는 국가정보원의 직무수행 과정에서 헌법기관인 중앙선거관리위원회가 대통령 소속인 국가정보원의 감독과 통제를 받게 되거나 정보시스템 및 데이터 관리의 보안성·자율성이 침해될 수 있다는 우려가 제기될 수 있으며, 국가정보원의 예방·대응 업무 대상기관으로 규정되지 아니한 국회, 법원, 헌법재판소 등 다른 헌법기관과의 형평성 문제를 함께 고려할 필요가 있어 보임.

중앙선거관리위원회는 개정안에 대하여 헌법기관으로서 독립적 직무수행 보장, 국회 및 법원·헌법재판소 등 타 헌법기관과의 형평성 등을 고려하여 정치권 및 폭넓은 국민의 공감대를 바탕으로 충분하고 심도있는 논의를 거쳐 결정할 사안으로 신중 검토 필요 의견을 제시하였음⁷⁾.

이에 따라 개정안의 심사에 있어서는 전문적·실효적인 사이버 침해사고 예방·대응 필요성이라는 개정안의 취지와 함께, 헌법기관의 독립성·자율성 침해 가능성 측면을 종합적으로 고려하여야 할 것으로 보이며,

예방·대응 업무 대상기관의 확대 이전에 헌법기관의 독립성과 자

6) 국가정보원, 「「국가정보원법 일부개정법률안(강선영의원 대표발의)」에 대한 국정원 의견」, 2025.

7) 중앙선거관리위원회, 「법률안 의견제시 요청 회신」, 2025.

울성을 침해하지 않는 범위에서 가능한 기관별 자체 보안관계 역량 제고, 사이버 위협 관련 정보 공유 강화, 기관 간 협의에 따른 선제적 취약요소 점검 실시 등을 시행하는 방안을 검토할 수 있어 보임.

또한 현행 법률체계를 보면, 「전자정부법」 제56조제3항은 행정기관의 장으로 하여금 정보통신망을 이용한 전자문서의 보관·유통 시 국가정보원장이 안전성을 확인한 보안조치를 하도록 하고 국가정보원장이 그 이행 여부를 확인할 수 있도록 하는 한편, 같은 조 제4항은 제3항을 적용할 때 헌법기관의 경우에는 해당 기관의 장이 필요하다고 인정하는 경우에만 적용되, 다만 필요하지 아니하다고 인정하는 경우에는 해당 기관의 장은 국가정보원장이 안전성을 확인한 보안조치에 준하는 보안조치를 마련하여야 한다고 규정하고 있음⁸⁾.

「국가정보원법」에 따른 국가정보원의 직무 규정이 개정되더라도 「전자정부법」이 개정되지 아니하면 헌법기관의 장이 필요성을 인정하는 경우에만 국가정보원장이 정보통신망을 이용한 전자문서의 보관·유통 관련 보안조치의 이행 여부 등을 확인할 수 있게 되어 있는 점을 감안하여 법률간 체계정합성을 검토할 필요가 있음.

이와 관련하여 국가정보원이 사이버공격 및 위협에 대한 예방 및

8) 「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.

대응 직무를 수행할 수 있는 기관에 “국회·법원·헌법재판소·선거관리위원회와 그 소속기관”을 추가하는 내용의 「국가정보원법 일부개정법률안」(유상범의원 대표발의)이 정보위원회 법안심사소위원회에 회부되어 있으며, 「전자정부법」 제56조제4항을 삭제하여 헌법상 독립기관에 대해서도 해당 기관의 필요성 인정 여부와 관계 없이 국가정보원장이 안전성을 확인한 보안조치를 하도록 하고 그 이행 여부를 확인할 수 있도록 하려는 내용의 「전자정부법 일부개정법률안」(유상범의원 대표발의)이 행정안전위원회에 계류 중임.

문 의 처
02) 6788-5614

※ 참고: 「사이버안보 업무규정」에 따른 예방·대응 업무 범위

제9조(사이버보안 예방 조치 등) ① 국가정보원장은 중앙행정기관등에 대한 사이버공격·위협을 예방하기 위하여 중앙행정기관등의 장이 시행하는 정보화사업(「지능정보화 기본법」 제11조제1항에 따른 지능정보화계획에 따른 사업을 포함한다)에 대하여 보안성 검토를 실시하고, 그 보안성 검토 결과의 이행 여부를 확인할 수 있다.

② 국가정보원장은 중앙행정기관등의 정보보호시스템, 암호장치, 암호모듈 및 보안기능이 있는 정보통신기기(이하 “정보보호시스템등”이라 한다)의 도입·운영 및 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제3호에 따른 클라우드컴퓨팅서비스(이하 이 조에서 “클라우드컴퓨팅서비스”라 한다)의 이용에 관한 보안대책을 수립할 수 있다.

③ 국가정보원장은 중앙행정기관등이 도입·운영하거나 이용하는 정보보호시스템등 및 클라우드컴퓨팅서비스가 제2항에 따른 보안대책에 적합한지 검증할 수 있다.

④ 국가정보원장은 정보보호시스템등을 직접 개발하여 중앙행정기관등에 보급할 수 있다.

⑤ 국가정보원장은 중앙행정기관등의 정보통신기기, 정보통신망 또는 이와 관련된 정보시스템의 취약요소를 발굴·개선하기 위해 보안관리 수준을 측정할 수 있다. 이 경우 그 항목·절차·시기 등을 해당 중앙행정기관등의 장에게 미리 통보해야 한다.

⑥ 제5항에도 불구하고 제7조 각 호에 따른 기관 중 국가정보원장과 국방부장관이 협의하여 정하는 기관에 대해서는 국방부장관이 보안관리 수준을 측정한다. 이 경우 국가안보에 필요하다고 판단되거나 국가정보원장의 요청이 있는 경우에는 관련 내용을 국가정보원장에게 통보해야 한다.

제13조(사이버보안 실태 평가) ① 국가정보원장은 중앙행정기관등의 사이버보안 업무 수행을 위한 조직, 인력, 예산, 직무교육 및 사이버보안에 대한 자체 진단·점검 등 사이버보안 실태를 평가할 수 있다.

② 국가정보원장은 제1항에 따른 평가를 하려는 경우 평가의 항목·절차·시기 등을 해당 중앙행정기관등의 장에게 미리 통보해야 한다.

③ 국가정보원장은 제1항에 따른 평가의 결과를 해당 중앙행정기관등의 장에게 통보해야 한다.

④ 제3항에 따라 평가 결과를 통보받은 해당 중앙행정기관등의 장은 평가의 결과에 따라 문제점이 발견된 경우에는 그 결과를 통보받은 날부터 3개월 이내에 개선대책을 마련하고 국가정보원장에게 통보해야 한다.

⑤ 국가정보원장은 중앙행정기관등의 장이 제4항에 따라 통보한 개선대책에 대한 이행 여부를 확인할 수 있다.

- ⑥ 국가정보원장은 국가안전보장에 지장이 없는 범위에서 제1항에 따른 실태 평가 결과를 공개할 수 있다.
- ⑦ 국가정보원장은 제1항에 따른 평가의 효율적 수행, 평가에 관한 전문적·기술적인 연구 등을 위하여 필요한 경우 관계 전문가를 활용할 수 있다.

제14조(통합보안관제) ① 국가정보원장은 중앙행정기관등에 대한 사이버공격·위협을 즉시 탐지·대응[이하 “보안관제(保安管制)”라 한다]하기 위하여 통합보안관제체계를 구축·운영해야 한다.

- ② 중앙행정기관등의 장은 해당 기관의 보안관제를 위하여 제1항에 따른 통합보안관제체계와 연계된 보안관제센터를 설치·운영해야 한다. 다만, 다른 기관이 운영하는 보안관제센터를 활용하는 것이 더 효율적인 경우에는 직접 설치하지 않고 다른 기관의 보안관제센터를 활용할 수 있다.
- ③ 국가정보원장은 제1항에 따른 통합보안관제체계를 활용하여 각 중앙행정기관등의 장과 합동으로 해당 중앙행정기관등에 대한 보안관제를 실시할 수 있다.
- ④ 국가정보원장은 제3항에 따른 보안관제를 위하여 법 제5조제1항에 따라 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제4호에 따른 클라우드컴퓨팅서비스 제공자에게 필요한 협조 또는 지원을 요청할 수 있다.
- ⑤ 제1항부터 제4항까지에서 규정한 사항 외에 보안관제센터의 설치·운영 및 그 밖에 필요한 사항은 국가정보원장이 관계 중앙행정기관의 장과 협의하여 정한다.

제15조(경보 발령) ① 국가정보원장은 중앙행정기관등에 대한 사이버공격·위협에 체계적으로 대응 및 대비하기 위하여 과급영향 및 피해규모 등을 고려하여 단계별로 경보를 발령할 수 있다. 이 경우 국가안보실장과 미리 협의해야 한다.

- ② 제1항에도 불구하고 제7조 각 호에 따른 기관 중 국가정보원장과 국방부장관이 협의하여 정하는 기관에 대해서는 국방부장관이 경보를 발령한다. 이 경우 국가안보에 필요하다고 판단되거나 국가정보원장의 요청이 있는 경우에는 관련 내용을 국가정보원장에게 통보해야 한다.
- ③ 국가정보원장, 국방부장관 및 다른 법령에 따라 사이버공격·위협에 대응 및 대비하기 위한 경보를 발령하는 중앙행정기관의 장은 국가 차원에서의 효율적인 경보 업무를 수행하기 위하여 경보 관련 정보를 경보 발령 전에 상호 교환해야 한다.

제16조(사고 조사) ① 국가정보원장은 중앙행정기관등에 대한 사이버공격·위협으로 사고가 발생한 경우 공격 주체 규명, 원인 분석 및 피해 내역 확인 등을 위한 조사를 실시할

수 있다. 다만, 제7조 각 호에 따른 기관 중 국가정보원장과 국방부장관이 협의하여 정하는 기관에 대해서는 국방부장관이 조사를 실시할 수 있다.

② 제1항에도 불구하고 국가정보원장 또는 국방부장관은 중앙행정기관등에 대한 사이버 공격·위협으로 인한 사고가 국제 및 국가배후 해킹조직 등의 위해 행위에 해당되지 않거나, 그 밖의 경미한 사고라고 판단될 경우 해당 중앙행정기관등의 장이 자체적으로 조사하게 할 수 있다.

③ 국가정보원장은 제1항 및 제2항에 따른 조사 결과 해당 사고로 유출된 것으로 판단되는 자료에 대하여 해당 중앙행정기관등의 장과 합동으로 국가안보, 국익 및 정부 정책에 미치는 영향을 평가할 수 있다.

④ 국가정보원장은 해당 중앙행정기관등의 장에게 제3항에 따른 국가안보, 국익 및 정부 정책에 미치는 영향을 최소화하기 위하여 필요한 조치를 할 것을 요청할 수 있다.

⑤ 국가정보원장은 사이버보안 업무의 수행과 관련하여 필요한 경우 중앙행정기관등의 장에게 제1항 단서 및 제2항에 따른 조사 결과, 제4항에 따른 조치 결과의 제출을 요청할 수 있다. 이 경우 요청을 받은 중앙행정기관등의 장은 정당한 사유가 없으면 그 요청에 따라야 한다.

