

의안번호	제 호	의결사항
의결연월일	2023. . . (제 회)	

사이버안보업무규정 일부개정령안

제출자	행정안전부장관()
제출연월일	2023. . .

법제처 심사 전

1. 의결주문

사이버안보업무규정 일부개정령안을 별지와 같이 의결한다.

2. 제안이유

2020. 12. 15. 「국가정보원법」 전부개정(법률 제17646호)에 따라 국가 전 영역에서의 국제 및 국가배후 해킹조직 등 사이버안보 관련 정보의 수집·작성·배포 및 관련 대응조치와 공공분야 대상 사이버공격에 대한 예방 및 대응 직무가 부여된 바 있음.

이와 관련 2020. 12. 31. 제정된 「사이버안보 업무규정(대통령령)」에는 해당 직무를 수행하기 위한 구체적인 사항이 일부 결여되어 있어 이를 합리적으로 정비하고자 하려는 것임

3. 주요내용

가. 「정부조직법」에 따른 국가정보원 직무체계(정보·보안 업무)에 맞춰, 사이버안보 업무를 사이버안보정보 업무와 사이버보안 업무로 구분(안 제2조제2호 및 제3호, 제2장 및 제3장 신설)

나. 「국가정보원법」에 이미 부여된 전 국가영역에서의 사이버안보 정보 직무수행에 관하여 유념해야 할 원칙을 명확하게 규정(안 제3조)

다. 사이버안보 업무에 관한 기획·조정 방식 명시(안 제3조의2)

라. 사이버안보정보 관련 직무수행에 필요한 조사·대응조치 방법 등 세부사항 명시 (안 제5조 및 제6조)

- 마. 국가정보원의 사이버공격·위협에 대한 예방·대응활동 대상으로 국가·공공기관 이용 민간 클라우드컴퓨팅서비스 영역이 포함됨을 명시(안 제7조의2)
- 바. 각급기관 직원 대상 직무역량·인식제고를 위한 교육과정에 전문기관·단체를 활용할 수 있도록 규정(안 제10조)
- 사. 사이버안보 관련 전략 등의 연구·개발을 위하여 학회·협회 등을 전문기관으로 지정할 수 있도록 규정(안 제17조)

4. 주요토의과제

없 음

5. 참고사항

- 가. 관계법령 : 생 략
- 나. 예산조치 : 별도조치 필요 없음
- 다. 합 의 : 관계부처 의견 조회 중
- 라. 기 타 : 1) 신·구조문대비표, 별첨
2) 입법예고(2023. 10. 27. ~ 12. 5.) 결과, 특기할 사항 없음
3) 행정규제 : 규제개혁위원회 사전 협의 결과, 이견 없음

대통령령 제 호

사이버안보 업무규정

사이버안보 업무규정 일부를 다음과 같이 개정한다.

제1조 중 “제4조제1항제1호마목, 같은 항 제4호 및 같은 조 제3항에 따라 국가정보원의 직무 중 사이버안보 관련 정보의 수집·작성·배포 및 사이버공격·위협에 대한 예방·대응 업무의 수행에 필요한 사항”을 “제4조에 따라 국가정보원의 직무 중 사이버안보 업무의 수행에 필요한 사항”으로 한다.

제2조 중 제1호 중 “서비스거부”를 “디도스(Distributed Denial of Service, DDoS)”으로 하고, 제2호를 제5호로 하며, 같은 조에 제1호, 제2호 및 제3호를 다음과 같이 신설한다.

1. “사이버안보 업무”란 「국가정보원법」(이하 “법”이라 한다) 및 이 영에 따라 수행하는 사이버안보정보에 관련된 업무와 사이버보안 업무를 말한다.
2. “사이버안보정보”란 법 제4조제1항제1호마목에 따른 국제 및 국가 배후 해킹조직 등이 자행하는 국가안보와 국익에 반하는 일체의 침해행위에 관한 정보를 말한다.
3. “사이버보안 업무”라 함은 국가·공공 기능 유지를 위하여 국가정보원장과 법 제4조제1항제4호 각 목의 기관(이하 “각급기관”이라

한다)의 장이 수행하는 다음 각 목의 직무를 말한다.

가. 법 제4조제1항제4호에 따른 예방 및 대응

나. 법 제4조제1항제2호에 따른 보안업무 중에서 전자적 방법에 의하여 수행되는 업무

다. 법 제4조제1항제6호에 따른 사항 중에서 위 가목 또는 나목과 관련되어 국가정보원장이 따로 정하는 사항

제3조의 제목을 “사이버안보 업무의 수행”에서 “사이버안보정보에 관련된 업무 수행 원칙”으로 하고, 제1항과 제3항을 각각 삭제하고, 제2항 “국가정보원은 사이버정보업무를 수행할 때 중앙행정기관등 외의 기관에 대해서는 개별 법령에 근거가 있거나 해당 기관의 명시적인 요청 또는 동의가 있는 경우를 제외하고는 해당 기관의 정보통신망에 대한 접근 시도나 사이버안보 관련 정보의 수집 등의 행위를 하면 안 된다.”를 “국가정보원장은 사이버안보정보에 관한 업무를 수행할 경우 법 제3조의 운영원칙 및 다른 법률에 따른 적법절차를 준수하여야 한다.”로 한다.

제3조의2를 다음과 같이 신설하고, 제목을 “사이버안보 업무의 기획·조정”으로 한다.

① 국가정보원장은 법 제4조제1항제5호에 따라 사이버안보 업무를 수행하기 위하여 필요한 다음 각 호의 지침등을 수립·시행한다.

1. 사이버안보정보 업무의 협력에 관한 지침

2. 각급기관을 대상으로 하는 사이버보안 기본지침

3. 각급기관을 대상으로 하는 사이버보안 대책

② 국가정보원장은 각급기관이 수행하는 사이버안보정보의 협력 및 사이버보안 업무에 대한 조정이 필요한 경우, 국가안보에 중대한 영향을 미치는 주요 사안에 대해서는 직접 조정하고, 그 밖의 사안에 대해서는 제1항제1호 및 제2호에 따른 지침으로 정하는 바에 따라 조정한다.

제4조제2항을 제4항으로 하고 “중앙행정기관등”을 “법 제5조제1항에 따른 국가기관이나 그 밖의 관계 기관 또는 단체”으로 하며, 같은 조에 제2항과 제3항을 다음과 같이 신설한다.

② 제1항에 따른 국가사이버안보센터에는 제6조의2제3항에 따른 민관 합동 통합 대응체계를 구축·운영을 수행하기 위한 전담 조직을 둘 수 있다.

③ 제1항에 따른 국가사이버안보센터에는 사이버안보 업무 수행에 관한 사항을 전문적으로 검토하기 위하여 관계 전문가로 구성된 자문단을 둘 수 있다.

제2장을 신설하고 제목을 “사이버안보정보에 관련된 업무”로 한다.

제5조의 제목을 “기관 간 협력체계 구축”에서 “정보협력체계 구축 등”으로 하고, “사이버정보업무를”를 “사이버안보정보의 수집·작성·배포 직무”로 하며, “중앙행정기관등”을 “법 제5조제1항에 따른 국가기관이나 그 밖의 관계 기관 또는 단체”으로 한다. “외국 정보·보안기관”을 “외국의 사이버안보 업무를 수행하는 기관(정보·보안기관을 포함한다)로 하고,

“할 수 있다”를 “· 운영할 수 있다”로 한다.

제5조의2부터 제5조의3를 다음과 같이 신설한다.

제5조의2(사이버안보정보 조사를 위한 자료제출 요구) 국가정보원장은 법 제5조제2항의 방식에 의하여 사이버안보정보의 수집에 필요한 조사를 실시하는 경우, 해당 정보가 수록·기재된 디지털 자료 등을 그 소유자·소지자 또는 보관자로부터 제출받을 수 있다. 다만, 전기통신사업자가 보관 중인 전기통신이용자의 통신사실확인자료에 대하여 제출받고자 하는 경우에는 「통신비밀보호법」 제13조의4에 따른다.

제5조의3(사이버안보정보의 작성) 국가정보원장은 법 제4조제1항제1호마목에 따라 수집한 국내의 정보를 종합·분석·평가하여 위해(危害) 행위의 수준, 국가안전보장에 미치는 영향, 그에 필요한 방어진치 등이 포함된 정보를 작성한다.

제6조의 제목을 “정보공유시스템 구축”에서 “사이버안보정보의 배포 등”으로 하고, 제1항 중 “사이버안보 관련 정보”를 “사이버안보정보”로, “중앙행정기관등”을 삭제하며, 제2항 중 “중앙행정기관등과 협의하여”를 “3조제1항제1호에 따른 지침으로”로 한다.

제6조의2를 다음과 같이 신설한다.

제6조의2(사이버안보정보에 관련된 대응조치 등) ① 국가정보원장은 법 제4조제1항제3호에 따라 국가안보와 국익에 반하는 활동에 악용되거나 악용될 만한 상당한 개연성이 있는 경우 정보통신기기·소프트웨어를 확인하기 위하여 기술적 시험·분석 등 검증할 수 있다. 검증결과에 따

라 국가정보원장은 위험 최소화 조치를 할 수 있는 법 제5조제1항에 따른 국가기관이나 그 밖의 관계 기관 또는 단체에게 조치를 요청할 수 있고, 해당 기관 또는 단체는 필요한 경우에는 국가정보원장에게 지원을 요청할 수 있다.

② 국가정보원장은 법 제4조제1항제3호에 따라 국가안보와 국익에 반하는 국제 및 국가배후 해킹조직 등의 활동을 선제적으로 확인·견제·차단하기 위하여 국외 및 북한을 대상으로 추적, 무력화 등 조치를 취할 수 있다.

③ 국가정보원장은 법 제4조제1항제3호에 따라 국가안보나 국익에 반하는 활동으로부터 국민안전 보호를 위하여 국가안보실장과 협의하여 위기상황을 관리하기 위한 민관 합동 통합대응 체계를 구축·운영할 수 있다.

제3장을 신설하고 제목을 “사이버보안 업무”로 한다.

제7조의 제목 중 “사이버공격예방·대응업무 대상 공공기관”을 “공공기관”으로 하고, 제목 외의 부분 중 “3. 특별법에 따라 설립된 특수법인 중 다음 각 목에 따른 법인 가. 「한국은행법」에 따른 한국은행 나. 「방송법」 제43조에 따른 한국방송공사 다. 「한국교육방송공사법」에 따른 한국교육방송공사 라. 「한국해운조합법」에 따른 한국해운조합”을 “특별법에 의하여 설립한 법인(다만, 「지방문화원진흥법」에 의한 문화원 및 특별법에 의하여 설립된 조합·협회를 제외한다.)”로 하고, 제2호2를 다음과 같이 신설한다.

2의2. 「지방자치단체 출자·출연 기관의 운영에 관한 법률」 제2조제1항에 따른 출자·출연기관 중 해당 지방자치단체의 조례로 정하는 기관

제7조의2를 다음과 같이 신설한다.

제7조의2(각급기관 대상 사이버공격·위협) 법 제4조제1항제4호에 따른 “각급기관 대상 사이버공격·위협”이란 다음 각 호와 같다.

1. 각급기관이 관리하는 정보통신기기, 정보시스템을 대상으로 하는 사이버공격·위협
2. 각급기관이 처리하는 행정정보(「전자정부법」 제2조제6호에 따른 행정정보를 말한다) 및 전자기록물(「공공기록물 관리에 관한 법률 시행령」 제2조에 따른 전자기록물을 말한다)을 대상으로 하는 사이버공격·위협
3. 「전자정부법」 제54조의2 및 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제20조에 따라 각급기관이 이용하는 클라우드컴퓨팅 서비스 이용영역(물리적, 논리적 영역을 포함한다)을 대상으로 하는 사이버공격·위협
4. 그 밖에 각급기관의 기능 유지에 지장을 초래할 우려가 있다고 각급기관의 장이 자체적으로 분류·판단한 사이버공격·위협

제8조의 제목을 “사이버안보 기본대책의 수립·시행등”을 “각급기관의 사이버안보 업무체계 구축 등”으로 하고, 제목 외의 부분 중 제1항을 삭제하며, 제2항 중 “중앙행정기관등의 장은 제1항에 따른 사이버안보 기본대

책”을 “각급기관의 장은 제3조제1항제2호에 따른 사이버보안 기본지침”으로 하고 “사이버안보 세부대책”을 “사이버보안 세부지침”으로 한다.

제9조의 제목을 “사이버공격·위협 예방 조치 등”을 “예방 조치 등”으로 하고, 제목 외의 부분 중 제1항 “중앙행정기관등에 대한”을 “각급기관 대상”으로 하고 “중앙행정기관등”을 “각급기관”으로 하며, 제2항 “중앙행정기관등”을 “각급기관”으로 하고 “암호모듈 및 보안기능이 있는 정보통신기기(이하 “정보보호시스템등”이라 한다)의 도입·운영”을 “암호모듈, 보안기능이 있는 정보통신기기 및 클라우드컴퓨팅서비스 이용영역(이하 “정보보호시스템등”이라 한다)의 도입·운영·이용”으로 한다. 또한, 제3항 “중앙행정기관등이 도입·운영”을 “각급기관이 도입·운영·이용”으로 하며, 제4항 “중앙행정기관등”을 “각급기관”으로 한다. 제5항 “중앙행정기관등과 협의하여 해당 중앙행정기관등”을 “각급기관”으로 하고, “개선하는 등 보안관리 컨설팅”을 “개선하기 위한 보안측정”으로 하며, 같은 항 후단으로 “이 경우 해당 각급기관의 장은 측정 결과를 통보받은 날로부터 3개월 이내에 국가정보원장에게 개선대책을 회신하여야 하며, 국가정보원장은 그 이행여부를 확인할 수 있다.”을 신설한다.

제10조의 제목을 “사이버공격·위협에 대한 예방·대응 교육”을 “사이버보안 직무교육”으로 하고, 제목 외의 부분 중 제1항 “중앙행정기관등의 장은 사이버 공격·위협에 대한 예방 및 대응 업무를 수행하는 소속 공무원 및 임직원의 직무역량을 높이기 위하여 필요한”을 “각급기관의 장은 소속 공무원 및 임직원의 직무역량 및 인식 제고를 위하여 사이버보안”으로 하

며, 후단에 “이 경우 사이버보안 교육내용·방법 등 그 밖에 필요한 사항은 국가정보원장이 별도 정할 수 있다.”를 신설한다. 제2항 “중앙행정기관등의 사이버 공격·위협에 대한 예방 및 대응 업무를 수행하는 공무원 및 임직원의 직무역량 향상을 지원하기 위하여”를 “제1항에 따른 교육을 지원하기 위하여”로 하고, 제3항을 다음과 같이 신설한다.

③ 국가정보원장은 제1항에 따른 직무역량 및 인식제고 및 제2항에 따른 교육과정의 운영을 위하여 그 밖의 지원이 필요하다고 판단하는 경우 이를 지원할 수 있다. [시행일 : 2025.1.1.]

제11조 제1항 중 “중앙행정기관등”을 “각급기관”으로 하고, “기관에 대한”을 “기관 대상”으로 하며, 제2항, 제3항 및 제4항 중 “중앙행정기관등”을 “각급기관”으로 한다.

제12조의 제목을 “사이버공격·위협에 대비한”을 “각급기관의”로 하고, 제1항 중 “중앙행정기관등”을 “각급기관”으로 하며, 제2항 “중앙행정기관등의 장이”를 삭제하고, “조치를 한 경우에는”을 “조치가 이루어진 경우에는”으로 하며, 같은 조 같은 항 제1호를 삭제하고 제3호 “보안관리 컨설팅”을 “국가정보원장이 실시한 보안측정”으로 하고, 제3항 “중앙행정기관등”을 “각급기관”으로 하며, 제4항을 다음과 같이 신설한다.

④ 국가정보원장은 사이버보안 업무 수행과 관련하여 필요한 경우 각급기관의 장에 대하여 제1항에 따른 진단·점검 결과 및 제4항에 따른 조치 결과를 요청할 수 있다. 이 경우 요청을 받은 각급기관의 장은 정당한 사유가 없으면 그 요청에 따라야 한다.

제13조의 제목 “사이버공격·위협에 대한 예방·대응” 부분을 삭제하고, 제1항을 다음과 같이 신설한다.

① 국가정보원장은 각급기관의 사이버보안 업무에 관한 조직, 인력, 예산, 직무교육, 자체점검 활동 등 현황을 종합·분석할 수 있으며, 필요한 경우 현장 확인을 할 수 있다. 이 경우 국가정보원장은 법 제5조제1항에 따라 각급기관의 장에게 자료의 제출을 요청할 수 있으며, 요청을 받은 각급기관의 장은 정당한 사유가 없으면 그 요청에 따라야 한다.

같은 조 제1항부터 제3항을 각각 제2항부터 제4항으로 하고, 제2항(종전 제1항) “중앙행정기관등”을 “위 제1항에 따른 각급기관의 사이버보안 업무 현황을 반영하여 각급기관”으로 하며, 제3항(종전 제2항) “중앙행정기관등”을 “각급기관”으로 한다. 같은 조 제4항(종전 제3항) “중앙행정기관등”을 “각급기관”으로 하고, 같은 항 후단으로 “이 경우 해당 각급기관의 장은 결과를 통보받은 날로부터 3개월 이내에 국가정보원장에게 개선대책을 통보해야 한다.”를 신설하며, 제5항부터 제7항까지 다음과 같이 신설한다.

⑤ 국가정보원장은 제4항에 따라 해당 각급기관의 장이 통보한 개선대책에 대한 이행여부를 확인할 수 있고, 필요한 경우 해당 각급기관의 장에게 시정 등 필요한 조치를 권고할 수 있다. 이 경우 국가정보원장은 필요한 경우 각급기관의 장에 대하여 조치 결과를 요청할 수 있고, 요청을 받은 각급기관의 장은 정당한 사유가 없으면 그 요청에 따라야 한다.

⑥ 국가정보원장은 국가안전보장에 지장이 없는 범위 내에서 제1항에

다른 종합·분석 결과와 제2항 및 제3항에 따른 평가 기준 및 결과를 공개할 수 있다.

⑦ 국가정보원장은 제2항부터 제6항에 따른 실태평가의 효율적인 수행과 실태평가에 관한 전문적·기술적인 연구 또는 자문을 위하여 민간 전문가 등을 위촉할 수 있다.

제14조의 제목 “사이버공격·위협·탐지·대응”을 “국가보안관제”로 하고, 제1항 “정부 차원에서”를 “각급기관 대상”으로 하며 “정부보안관제체계”를 “국가보안관제체계”로 한다. 같은 조 제2항 및 제3항의 “중앙행정기관등”을 “각급기관”으로 하고, “정부보안관제체계”를 “국가보안관제체계”로 하며, 제4조를 다음과 같이 신설한다.

④ 국가정보원장은 제7조의2제3호에 따른 사이버공격·위협에 대한 보안관제를 위하여 법 제5조제1항에 따라 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제4호에 따른 클라우드컴퓨팅서비스 제공자에게 필요한 협조 또는 지원을 요청할 수 있다. 이 경우 요청을 받은 클라우드컴퓨팅서비스 제공자는 정당한 사유가 없으면 그 요청에 따라야 한다.

같은 조 제4항을 제5항으로 하고, 제5항(종전 제4항) “제1항부터 제3항”을 “제1항부터 제4항”으로 한다.

제15조 제1항 “중앙행정기관등에 대한”을 “각급기관 대상”으로 하고, 제2항은 삭제하며, 제3항 “, 과학기술정보통신부장관 및 국방부장관은”을 “과 중앙행정기관의 장은 제1항과 동일한 원인으로 다른 법령에 따라 각급기

관 외의 기관·단체에 정보를 발령하려는 경우”로 한다.

제16조 제1항 및 제2항 “중앙행정기관등에 대한”을 “각급기관 대상”으로 하고, 제2항부터 제4항까지 “중앙행정기관등”을 “각급기관”으로 하며, 제5항을 다음과 같이 신설한다.

⑤ 국가정보원장은 사이버보안 업무 수행과 관련하여 필요한 경우 각급기관의 장에 대하여 제2항에 따른 조사 결과 및 제4항에 따른 조치 결과를 요청할 수 있다. 이 경우 요청을 받은 각급기관의 장은 정당한 사유가 없으면 그 요청에 따라야 한다.

제4장을 신설하고 제목을 “보칙”으로 한다.

제17조 제2항 “연구·개발”을 “연구·개발(연구개발을 위하여 보안관제, 보안측정을 수행하는 것을 포함한다)”로 하고, “「과학기술분야 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조제1항에 따라 설립된 연구기관 등”을 “학회, 학술단체 등 비영리법인, 「과학기술분야 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조제1항에 따라 설립된 연구기관 등”으로 하며, 같은 조 제3항을 제4항으로 하고 제3항을 다음과 같이 신설한다.

③ 국가정보원장은 제2항에 따른 전문기관을 지정하기 위하여 지정기준·절차 및 지정방법 등에 필요한 세부사항을 정한다.

제18조 “및 중앙행정기관등”을 “또는 각급기관”으로 하고, 같은 조 제1호 “사이버정보업무의 수행을 위한”을 “사이버안보정보 수집을 위하여 필요한”으로 한다.

제19조 및 제20조를 다음과 같이 신설한다.

제19조(권한의 위탁) ① 국가정보원장은 제7조 각 호 기관 중에서 국방부 산하 기관 및 방위사업청 산하 기관에 대한 다음 각 호 권한 일부를 국방부장관에게 위탁할 수 있다.

1. 제9조제5항에 따른 보안측정
2. 제15조제1항에 따른 정보발령
3. 제16조제1항에 따른 사고조사

② 국방부장관은 제1항에 따른 업무를 수행함에 있어 국가안보에 필요하다고 판단되거나 국가정보원장의 요청이 있는 경우에는 관련 내용을 국가정보원장에게 통보하여야 한다.

제20조(하부규정 위임) 이 영의 시행에 필요한 세부사항은 국가정보원장이 따로 정한다.

부 칙

제1조(시행일) 이 영은 공포한 날부터 시행한다. 다만, 제10조제1항 및 제3항의 개정규정은 2025. 1. 1.부터 시행한다.

신·구조문대비표

현행	개정안
<章 신설>	제1장 총칙
제1조(목적) 이 영은 「국가정보원법」 제4조제1항제1호마목, 같은 항 제4호 및 같은 조 제3항에 따라 국가정보원의 직무 중 사이버안보 관련 정보의 수집·작성·배포 및 사이버공격·위협에 대한 예방·대응 업무의 수행에 필요한 사항을 규정함을 목적으로 한다.	제1조(목적) ----- -- 제4조에 따라 국가정보원의 직무 중 사이버안보 업무의 수행에 필요한 사항 -----.
제2조(정의) 이 영에서 사용하는 용어의 뜻은 다음과 같다.	제2조(정의) ----- -----. 1. “사이버안보 업무”란 「국가정보원법」(이하 “법”이라 한다) 및 이 영에 따라 수행하는 사이버안보정보에 관련된 업무와 사이버보안 업무를 말한다. 2. “사이버안보정보”란 법 제4조제1항제1호마목에 따른 국제 및 국가배후 해킹조직 등이 자행하는 국가안보와 국익에 반하는 일체의 침해행위에 관한 정보를

현행	개정안
	말한다. 3. “사이버보안 업무”라 함은 국가·공공 기능 유지를 위하여 국가정보원장과 법 제4조제1항 제4호 각 목의 기관(이하 “각급 기관”이라 한다)의 장이 수행하는 다음 각 목의 직무를 말한다. 가. 법 제4조제1항제4호에 따른 예방 및 대응 나. 법 제4조제1항제2호에 따른 보안업무 중에서 전자적 방법에 의하여 수행되는 업무 다. 법 제4조제1항제6호에 따른 사항중에서 위 가목 또는 나목과 관련되어 국가정보원장이 따로 정하는 사항 4. ----- ----- ----- -----
1. “정보통신망”이란 「전기통신사업법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용	

현행	개정안
기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말한다. 2. “사이버공격·위협”이란 해킹, 컴퓨터 바이러스, 서비스거부, 전자파 등 전자적 수단에 의하여 정보통신기기, 정보통신망 또는 이와 관련된 정보시스템을 침입·교란·마비·파괴하거나 정보를 위조·변조·훼손·절취하는 행위 및 그와 관련된 위협을 말한다.	----- ----- -----. 5. ----- ----- 디도스(Distributed Denial of Service, DDOS), ----- ----- ----- ----- -----.
제3조(사이버안보 업무의 수행)	제3조(사이버안보정보에 관련된 업무 수행 원칙)
① 국가정보원은 사이버안보를 위하여 다음 각 호의 업무(이하 “사이버안보 업무”라 한다)를 수행한다. 1. 「국가정보원법」(이하 “법”이라 한다) 제4조제1항제1호마목에 따른 국제 및 국가배후 해킹 조직 등 사이버안보 관련 정보의 수집·작성·배포 업무(이하 “사	<삭제>

현행	개정안
<u>이버정보업무</u>”라 한다) 2. 법 제4조제1항제4호 각 목의 기 관(이하 “중앙행정기관등”이라 한다)을 대상으로 하는 사이버 공격·위협에 대한 예방 및 대응 업무(이하 “사이버공격예방·대 응업무”라 한다) ② 국가정보원은 사이버정보업무를 수행할 때 중앙행정기관등 외의 기 관에 대해서는 개별 법령에 근거가 있거나 해당 기관의 명시적인 요청 또는 동의가 있는 경우를 제외하고 는 해당 기관의 정보통신망에 대한 접근 시도나 사이버안보 관련 정보 의 수집 등의 행위를 하면 안 된다. ③ 국가정보원은 사이버공격예방· 대응업무를 수행할 때 해당 중앙행 정기관등의 정보통신망이 「정보통 신기반 보호법」에 따른 주요정보 통신기반시설인 경우에는 「정보통	국가정보원장은 사이버안보정보 에 관한 업무를 수행할 경우 법 제3조의 운영원칙 및 다른 법률에 따른 적법절차를 준수하여야 한 다. <삭제>

현행	개정안
<u>신기반 보호법」을 우선 적용해야 한다.</u> <조 신설>	제3조의2(사이버안보 업무의 기획 · 조정) ① 국가정보원장은 법 제4조제1 항제5호에 따라 사이버안보 업무 를 수행하기 위하여 필요한 다음 각 호의 지침등을 수립·시행한 다. 1. 사이버안보정보 업무의 협력 에 관한 지침 2. 각급기관을 대상으로 하는 사 이버보안 기본지침 3. 각급기관을 대상으로 하는 사 이버보안 대책 ② 국가정보원장은 각급기관이 수 행하는 사이버안보정보의 협력 및 사이버보안 업무에 대한 조정이 필요한 경우, 국가안보에 중대한 영향을 미치는 주요 사안에 대해 서는 직접 조정하고, 그 밖의 사안

현행	개정안
	에 대해서는 제1항 제1호 및 제2호에 따른 지침으로 정하는 바에 따라 조정한다.
제4조(국가사이버안보센터) ① 국가정보원장은 사이버안보 업무를 효율적으로 수행하기 위하여 국가사이버안보센터를 둘 수 있다.	제4조(국가사이버안보센터) ①----- ----- ----- ② 제1항에 따른 국가사이버안보센터에는 제6조의2제3항에 따른 민관 합동 통합 대응체계를 구축·운명을 수행하기 위한 전담 조직을 둘 수 있다. ③ 제1항에 따른 국가사이버안보센터에는 사이버안보 업무 수행에 관한 사항을 전문적으로 검토하기 위하여 관계 전문가로 구성된 자문단을 설치하여 운영할 수 있다. ④ ----- ----- ----- 법 제5조제1항에 따른 국가기관이나 그 밖의
② 국가정보원장은 제1항에 따른 국가사이버안보센터의 운영을 위하여 필요한 경우 중앙행정기관등의 장에게 소속 공무원 또는 임직원의	

현행	개정안
파견 등 협조를 요청할 수 있다.	관계 기관 또는 단체----- -----.
<章 신설>	제2장 사이버안보정보에 관련된 업무
제5조(기관 간 협력체계 구축) 국가정보원장은 사이버정보업무의 수행을 위하여 필요한 경우 중앙행정기관등 및 외국 정보·보안기관과 정보협력체계를 구축할 수 있다.	제5조(정보협력체계 구축등) ----- ----- 사이버안보정보의 수집·작성·배포 직무 ----- ----- 법 제5조제1항에 따른 국가기관이나 그 밖의 관계 기관 또는 단체 - 외국의 사이버안보 업무를 수행하는 기관(정보·보안기관을 포함한다) ----- -----·운영할 수 있다.
<조 신설>	제5조의2(사이버안보정보 조사를 위한 자료제출 요구) 국가정보원장은 법 제5조제2항의 방식에 의하여 사이버안보정보의 수집에 필요한 조사를 실시하는 경우, 해당 정보가 수록·기재된 디지털 자료 등을 그 소유자·소지자 또는 보관자로부터 제출받을 수

현행	개정안
	있다. 다만, 전기통신사업자가 보 관 중인 전기통신이용자의 통신 사실확인자료에 대하여 제출받 고자 하는 경우에는 「통신비밀 보호법」 제13조의4에 따른다.
<조 신설>	제5조의3(사이버안보정보의 작성) 국가정보원장은 법 제4조제1항제 1호마목에 따라 수집한 국내외 정보를 종합·분석·평가하여 위 해(危害) 행위의 수준, 국가안전 보장에 미치는 영향, 그에 필요한 방어조치 등이 포함된 정보를 작 성한다.
제6조(정보공유시스템 구축) ① 국가 정보원장은 <u>사이버안보 관련 정보</u> 를 중앙행정기관등에 배포·공유 하기 위하여 정보공유시스템을 구 축·운영할 수 있다. ② 제1항에 따른 정보공유시스템의 활용 대상 및 범위 등 운영에 필요 한 사항은 국가정보원장이 관계 중	제6조(사이버안보정보의 배포 등) ① ----- <u>사이버안보정</u> <u>보를</u> ----- ----- -----. ② ----- ----- ----- 제

현행	개정안
<u>양행정기관등과 협의하여</u> 정한다. <조 신설>	3조제1항제1호에 따른 지침으로- -----. 제6조의2(사이버안보정보에 관련 된 대응조치 등) ① 국가정보원 장은 법 제4조제1항제3호에 따 라 국가안보와 국익에 반하는 활 동에 악용되거나 악용될 만한 상 당한 개연성이 있는 경우 정보통 신기기·소프트웨어를 확인하기 위하여 기술적 시험·분석 등 검 증할 수 있다. 검증결과에 따라 국가정보원장은 위험 최소화 조 치를 할 수 있는 법 제5조제1항 에 따른 국가기관이나 그 밖의 관계 기관 또는 단체에게 조치를 요청할 수 있고, 해당 기관 또는 단체는 필요한 경우에는 국가정 보원장에게 지원을 요청할 수 있 다. ② 국가정보원장은 법 제4조제1 항제3호에 따라 국가안보와 국익

현행	개정안
	에 반하는 국제 및 국가배후 해킹 조직 등의 활동을 선제적으로 확인·견제·차단하기 위하여 국외 및 북한을 대상으로 추적, 무력화 등 공세적 조치를 할 수 있다. ③ 국가정보원장은 법 제4조제1항제3호에 따라 국가안보나 국익에 반하는 활동으로부터 국민안전 보호를 위하여 국가안보실장과 협의하여 위기상황을 관리하기 위한 민관 합동 통합대응 체계를 구축·운영할 수 있다.
<章 신설>	제3장 사이버보안 업무
제7조(사이버공격예방·대응업무 대상 공공기관의 범위) 법 제4조제1항제4호다목에서 “대통령령으로 정하는 공공기관”이란 다음 각 호의 기관을 말한다.	제7조(공공기관의 범위) -----
1. 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관	-----
2. 「지방공기업법」에 따른 지방	-----

현행	개정안
공사 및 지방공단	-----
3. 특별법에 따라 설립된 특수법인 중 다음 각 목에 따른 법인가. 「한국은행법」에 따른 한국은행	2의2. 「지방자치단체 출자·출연 기관의 운영에 관한 법률」 제2조제1항에 따른 출자·출연 기관 중 해당 지방자치단체의 조례로 정하는 기관 3. 특별법에 의하여 설립한 법인(다만, 「지방문화원진흥법」에 의한 문화원 및 특별법에 의하여 설립된 조합·협회를 제외한다.)
나. 「방송법」 제43조에 따른 한국방송공사	
다. 「한국교육방송공사법」에 따른 한국교육방송공사	
라. 「한국해운조합법」에 따른 한국해운조합	
4. 「초·중등교육법」, 「고등교육법」 및 그 밖의 다른 법률에 따라 설치된 국립·공립 학교	4. -----
5. 「정부출연연구기관 등의 설립	5. -----

현행	개정안
· 운영 및 육성에 관한 법률」	-----
제8조제1항 및 「과학기술분야	-----
정부출연연구기관 등의 설립·	-----
운영 및 육성에 관한 법률」 제	-----
8조제1항에 따른 연구기관	-----
<조 신설>	제7조의2(각급기관 대상 사이버공 격·위협) 법 제4조제1항제4호 에 따른 “각급기관 대상 사이버 공격·위협”이란 다음 각 호와 같다. 1. 각급기관이 관리하는 정보통 신기기, 정보시스템을 대상으 로 하는 사이버공격·위협 2. 각급기관이 처리하는 행정정 보(「전자정부법」 제2조제6호에 따른 행정정보를 말한다) 및 전자기록물(「공공기록물 관리 에 관한 법률 시행령」 제2조에 따른 전자기록물을 말한다)을 대상으로 하는 사이버공격· 위협

현행	개정안
	3. 전자정부법 제54조의2 및 「클라우드컴퓨팅 발전 및 이 용자 보호에 관한 법률」 제20 조에 따라 각급기관이 이용하 는 클라우드컴퓨팅서비스 이용 영역(물리적, 논리적 영역을 포 함한다)을 대상으로 하는 사이 버공격·위협 4. 그 밖에 각급기관의 기능 유 지에 지장을 초래할 우려가 있 다고 각급기관의 장이 자체적 으로 분류·판단한 사이버공격 ·위협
제8조(사이버안보 기본대책의 수립 · 시행 등) ① 국가정보원장은 국 가안보실장 및 관계 중앙행정기관 의 장과 협의하여 중앙행정기관등 에 대한 사이버공격예방·대응업무 를 효율적·체계적으로 수행하기 위하여 사이버안보 기본대책을 수 립·시행해야 한다.	제8조(각급기관의 사이버보안 업무 체계 구축 등) ① <삭제>

현행	개정안
② 중앙행정기관등의 장은 제1항에 따른 사이버안보 기본대책에 따라 해당 기관의 특성 및 보안 수준 등을 반영하여 해당 기관을 대상으로 한 사이버안보 세부대책을 수립·시행해야 한다.	② 각급기관의 장은 제3조제1항 제2호에 따른 사이버보안 - 지침 ----- 사이버보안 세부지침-----.
제9조(사이버공격·위협 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.	제9조(예방 조치 등) ① ----- 각급기관 대상 ----- 각급기관-----관-----
② 국가정보원장은 중앙행정기관등의 정보보호시스템, 암호장치, 암호모듈 및 보안기능이 있는 정보통신기기	② ----- 각급기관----- 보안기능이 있는 정보통신기기 및 클라우드컴퓨팅서비스 이용영역-----
(이하 “정보보호시스템등”	

현행	개정안
이라 한다)의 도입·운영에 관한 보안대책을 수립할 수 있다.	---- 도입·운영·이용-----.
③ 국가정보원장은 중앙행정기관등이 도입·운영하는 정보보호시스템등이 제2항에 따른 보안대책에 적합한지 검증할 수 있다.	③ ----- 각급기관이 도입·운영·이용-----.
④ 국가정보원장은 정보보호시스템등을 직접 개발하여 중앙행정기관등에 보급할 수 있다.	④ ----- 각급기관-----.
⑤ 국가정보원장은 중앙행정기관등과 협의하여 해당 중앙행정기관등의 정보통신기기, 정보통신망 또는 이와 관련된 정보시스템의 취약요소를 발굴·개선하는 등 보안관리 컨설팅을 할 수 있다.	⑤ ----- 각급기관-----기 위한 보안추정----- 이 경우 해당 각급기관의 장은 추정 결과를 통보받은 날로부터 3개월 이내에 국가정보원장에게 개선대책을 회신하여야 하며, 국가정보원장은 그 이행여부를 확인할 수 있다.
제10조(사이버공격·위협에 대한 예	제10조(사이버보안 직무교육)

현행	개정안
방·대응 교육) ① <u>중앙행정기관등</u> 의 장은 <u>사이버 공격·위협에 대한</u> <u>예방 및 대응 업무를 수행하는 소</u> <u>속 공무원 및 임직원의 직무역량을</u> <u>높이기 위하여 필요한 교육을 실시</u> <u>해야 한다.</u> ② 국가정보원장은 중앙행정기관등 의 <u>사이버 공격·위협에 대한 예방</u> <u>및 대응 업무를 수행하는 공무원 및</u> <u>임직원의 직무역량 향상을 지원하</u> <u>기 위하여</u> 관련 교육과정을 직접 운 영하거나 다른 기관·단체가 운영 하는 교육과정을 직무역량 교육과 정으로 지정할 수 있다.	① <u>각급기관-</u> ---- <u>소속 공무원 및 임직원의</u> <u>직무역량 및 인식 제고를 위하여</u> <u>사이버보안</u> ----- ----- <u>. 이 경우 사이버보안 교</u> <u>육내용·방법 등 그 밖에 필요한</u> <u>사항은 국가정보원장이 별도 정</u> <u>할 수 있다.[시행일 : 2025.1.1.]</u> ② ----- 제1항에 따른 <u>교육을 지원하기 위하여</u> ----- ----- ----- -----. ③ <u>국가정보원장은 제1항에 따른</u> <u>직무역량 및 인식제고 및 제2항에</u> <u>따른 교육과정의 운영을 위하여</u>

현행	개정안
	<u>그 밖의 지원이 필요하다고 판단</u> <u>하는 경우 이를 지원할 수 있다.</u> [시행일 : 2025.1.1.]
제11조(사이버공격·위협 대응 훈 련) ① <u>중앙행정기관등의 장은 매</u> <u>년 해당 기관에 대한 사이버공격·</u> <u>위협에 대응하기 위한 훈련을 실시</u> <u>해야 한다.</u> ② 국가정보원장은 국가안보실장과 협의하여 <u>중앙행정기관등에 대한</u> <u>사이버공격·위협에 대비한 통합</u> <u>훈련을 실시할 수 있다.</u> ③ 국가정보원장은 제2항에 따른 통합 훈련을 실시하려는 경우 특별 한 사유가 없으면 사전에 훈련 일정 등을 해당 <u>중앙행정기관등의 장에</u> <u>게 통보해야 한다.</u> ④ 국가정보원장은 제2항에 따른 통합 훈련 결과 필요하다고 판단하 는 경우에는 해당 <u>중앙행정기관등</u> <u>의 장에게</u> 시정조치를 요청할 수 있	제11조(사이버공격·위협 대응 훈 련) ① <u>각급기관</u>----- ----- <u>대상</u> ----- -----. ② ----- ----- <u>각급기관</u>----- -----. ③ ----- ----- ----- <u>각급기관</u>----- -----. ④ ----- ----- ----- <u>각급기관</u>--- -----

현행	개정안
다.	-.
⑤ 제1항에 따른 훈련 및 제2항에 따른 통합 훈련의 범위와 세부 내용에 관하여 필요한 사항은 국가정보원장이 정한다.	⑤ ----- ----- ----- -----.
제12조(사이버공격·위협에 대비한 진단·점검) ① 중앙행정기관등의 장은 해당 기관에 대한 사이버공격·위협에 대한 예방 및 대응에 필요한 진단·점검을 연 1회 이상 실시해야 한다.	제12조(각급기관의 진단·점검) ① 각급기관----- ----- ----- -----.
② 제1항에도 불구하고 중앙행정기관등의 장이 다음 각 호의 어느 하나에 해당하는 조치를 한 경우에는 제1항에 따른 진단·점검을 실시한 것으로 본다.	② ----- -----가 이루어진 경우에는 ----- -----,
1. 「보안업무규정」 제40조에 따른 정보통신보안감사	1. <삭제>
2. 「정보통신기반 보호법」 제9조에 따른 취약점 분석·평가	2. ----- -----
3. 제9조제5항에 따른 보안관리	3. ----- 국가정

현행	개정안
컨설팅	보원장이 실시한 보안측정
③ 중앙행정기관등의 장은 제1항에 따른 진단·점검 결과 취약요소가 발견된 경우 이를 시정하는 등 필요한 조치를 해야 한다.	③ 각급기관----- ----- ----- -----.
	④ 국가정보원장은 사이버보안 업무를 수행과 관련하여 필요한 경우 각급기관의 장에 대하여 제1항에 따른 진단·점검 결과 및 제4항에 따른 조치 결과를 요청할 수 있다. 이 경우 요청을 받은 각급기관의 장은 정당한 사유가 없으면 그 요청에 따라야 한다.
제13조(사이버공격·위협에 대한 예방·대응 실태 평가)	제13조(실태 평가) ① 국가정보원장은 각급기관의 사이버보안 업무에 관한 조직, 인력, 예산, 직무교육, 자체점검 활동 등 현황을 종합·분석할 수 있으며, 필요한 경우 현장 확인을 할 수 있다. 이 경우 국가정보원장은 법 제5조제1항에 따라 각급기관의

현행	개정안
	<u>장에게 자료의 제출을 요청할 수 있으며, 요청을 받은 각급기관의 장은 정당한 사유가 없으면 그 요청에 따라야 한다.</u>
① 국가정보원장은 <u>중앙행정기관등</u> 의 사이버공격 · 위협에 대한 예방 및 대응 실태 를 평가할 수 있다.	② ----- 위 제1항에 따른 각 급기관의 사이버보안 업무 현황을 <u>반영하여 각급기관-----</u> -----.
② 국가정보원장은 제1항에 따른 평가를 하려는 경우 평가의 항목· 절차· 시기 등을 해당 <u>중앙행정기</u> <u>관등</u>의 장에게 미리 통보해야 한다.	③ ----- ----- ----- <u>각급기관-</u> -----.
③ 국가정보원장은 <u>제1항</u>에 따른 평가의 결과를 해당 <u>중앙행정기관</u> <u>등</u>의 장에게 통보해야 한다.	④ ----- <u>제2항</u>----- - ----- <u>각급기</u> <u>관</u>-----. 이 경 우 해당 각급기관의 장은 결과를 통보받은 날로부터 3개월 이내에 <u>국가정보원장에게 개선대책을 통</u> <u>보해야 한다.</u>

현행	개정안
	⑤ 국가정보원장은 제4항에 따라 해당 각급기관의 장이 통보한 개 선대책에 대한 이행여부를 확인할 수 있고, 필요한 경우 해당 각급기 관의 장에게 시정 등 필요한 조치 를 권고할 수 있다. 이 경우 국가정 보원장은 필요한 경우 각급기관의 장에 대하여 조치 결과를 요청할 수 있고, 요청을 받은 각급기관의 장은 정당한 사유가 없으면 그 요 청에 따라야 한다.
	⑥ 국가정보원장은 국가안전보장 에 지장이 없는 범위 내에서 제1항 에 따른 종합·분석 결과와 제2항 및 제3항에 따른 평가 기준 및 결 과를 공개할 수 있다.
	⑦ 국가정보원장은 제2항부터 제6 항에 따른 실태평가의 효율적인 수 행과 실태평가에 관한 전문적·기 술적인 연구 또는 자문을 위하여

현행	개정안
	민간 전문가 등을 위촉할 수 있다.
제14조(사이버공격·위협에 탐지·	제14조(국가보안관제)
대응) ① 국가정보원장은 정부 차	① -----각급기
원에서 사이버공격·위협을 즉시	관 대상 -----
탐지·대응[이하 “보안관제(保安	-----
管制)”라 한다]하기 위하여 정부보	-----국가-
안관제체계를 구축·운영해야 한	-----
다.	-.
② 중앙행정기관등의 장은 해당 기	② <u>각급기관</u> -----
관의 보안관제를 위하여 제1항에	-----
따른 정부보안관제체계와 연계된	----국가-----
보안관제센터를 설치·운영해야 한	-----
다. 다만, 다른 기관이 운영하는 보	-----
안관제센터를 활용하는 것이 더 효	-----
율적인 경우에는 직접 설치하지 않	-----
고 다른 기관의 보안관제센터를 활	-----
용할 수 있다.	-----,
③ 국가정보원장은 제1항에 따른	③ -----
정부보안관제체계를 활용하여 각	국가-----
중앙행정기관등의 장과 합동으로	각급기관-----
해당 중앙행정기관등에 대한 보안	----각급기관-----

현행	개정안
관제를 실시할 수 있다.	-----.
	④ 국가정보원장은 제7조의2제3
	호에 따른 사이버공격·위협에 대
	한 보안관제를 위하여 법 제5조제
	1항에 따라 「클라우드컴퓨팅 발전
	및 이용자 보호에 관한 법률」 제2
	조제4호에 따른 클라우드컴퓨팅서
	비스 제공자에게 필요한 협조 또는
	지원을 요청할 수 있다. 이 경우 요
	청을 받은 클라우드컴퓨팅서비스
	제공자는 정당한 사유가 없으면 그
	요청에 따라야 한다.
④ 제1항부터 제3항까지에서 규정	⑤ -----제4항-----
한 사항 외에 보안관제센터의 설치	-----
· 운영 및 그 밖에 필요한 사항은	-----
국가정보원장이 관계 중앙행정기관	-----
의 장과 협의하여 정한다.	-----.
제15조(경보 발령) ① 국가정보원장	제15조(경보 발령) ① -----
은 중앙행정기관등에 대한 사이버	---- <u>각급기관 대상</u> -----
공격·위협에 체계적으로 대응 및	-----
대비하기 위하여 과급영향 및 피해	-----

현행	개정안
규모 등을 고려하여 단계별로 경보를 발령할 수 있다. 이 경우 국가안보실장과 미리 협의해야 한다. ② 제1항에도 불구하고 민간분야에 대해서는 과학기술정보통신부장관이 경보를 발령하고, 국방분야에 대해서는 국방부장관이 경보를 발령한다. ③ 국가정보원장, 과학기술정보통신부장관 및 국방부장관은 국가 차원에서의 효율적인 정보 업무를 수행하기 위하여 정보 관련 정보를 정보 발령 전에 상호 교환해야 한다.	----- ----- -----. ② <삭제> ③ 국가정보원장과 중앙행정기관의 장은 제1항과 동일한 원인으로 다른 법령에 따라 각급기관 외의 기관·단체에 정보를 발령하려는 경우 ----- ----- ----- -----.
제16조(사고 조사) ① 국가정보원장은 중앙행정기관등에 대한 사이버 공격·위협으로 사고가 발생한 경우 공격 주체 규명, 원인 분석 및 피해 내역 확인 등을 위한 조사를 실시할 수 있다.	제16조(사고 조사) ① ----- -- <u>각급기관 대상</u> ----- ----- ----- ----- -----.

현행	개정안
② 제1항에도 불구하고 국가정보원장은 중앙행정기관등에 대한 사이버 공격·위협으로 인한 사고가 국제 및 국가배후 해킹조직 등의 위해(危害) 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.	② ----- ----- <u>각급기관 대상</u> ----- ----- ----- ----- ----- ----- <u>각급기관</u> ----- -----. ③ ----- ----- ----- ----- ----- <u>각급기관</u> ----- ----- ----- -----. ④ ----- <u>각급기관</u> ----- ----- ----- ----- -----.

현행	개정안
	⑤ 국가정보원장은 사이버보안 업무 수행과 관련하여 필요한 경우 각급기관의 장에 대하여 제2항에 따른 조사 결과 및 제4항에 따른 조치 결과를 요청할 수 있다. 이 경우 요청을 받은 각급기관의 장은 정당한 사유가 없으면 그 요청에 따라야 한다.
<章 신설>	제4장 보칙
제17조(사이버안보 업무 관련 전략 등의 연구·개발) ① 국가정보원장은 사이버안보 업무의 수행에 필요한 전략·정책 및 기술을 연구·개발할 수 있다.	제17조(사이버안보 업무 관련 전략 등의 연구·개발) ①-----
② 국가정보원장은 제1항에 따른 연구·개발	② -----
을 위하여 「과학기술분야 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」	연구·개발(연구개발을 위하여 보안관계, 보안측정을 수행하는 것을 포함한다)----- 학회, 학술단체 등 비영리법인, -----

현행	개정안
제8조제1항에 따라 설립된 연구기관 등을 전문기관으로 지정할 수 있다.	----- ----- --.
③ 국가정보원장은 제2항에 따라 지정된 전문기관의 업무 수행을 위하여 그 필요한 경비의 전부 또는 일부를 예산의 범위에서 지원할 수 있다.	③ 국가정보원장은 제2항에 따른 전문기관을 지정하기 위하여 지정 기준·절차 및 지정방법 등에 필요한 세부사항을 정한다. ④ ----- ----- ----- ---
제18조(고유식별정보의 처리) 국가정보원장 및 중앙행정기관등의 장은 다음 각 호의 업무를 수행하기 위하여 불가피한 경우 「개인정보 보호법 시행령」 제19조제1호 또는 제4호에 따른 주민등록번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다.	제18조(고유식별정보의 처리)----- 또는 각급기관----- ----- ----- ----- ----- ----- -----.
1. 법 제5조제2항에 따른 사이버	1. ----- 사이버

현행	개정안
정보업무의 수행을 위한 조사 업무	안보정보 수집을 위하여 필요 한 -----
2 제16조에 따른 사고 조사 업무	2. -----
	제19조(권한의 위탁) ① 국가정보 원장은 제7조 각 호 기관 중에서 국방부 산하 기관 및 방위사업청 산하 기관에 대한 다음 각 호 권 한 일부를 국방부장관에게 위탁 할 수 있다. 1. 제9조제5항에 따른 보안측정 2. 제15조제1항에 따른 경보발 령 3. 제16조제1항에 따른 사고조 사 ② 국방부장관은 제1항에 따른 업 무를 수행함에 있어 국가안보에 필 요하다고 판단되거나 국가정보원 장의 요청이 있는 경우에는 관련 내용을 국가정보원장에게 통보하 여야 한다.
	제20조(하부규정 위임) 이 영의 시

현행	개정안
	행에 필요한 세부사항은 국가정 보원장이 따로 정한다.
	부 칙 제1조(시행일) 이 영은 공포한 날부 터 시행한다. 다만, 제10조제1항 및 제3항의 개정규정은 2025. 1. 1.부터 시행한다.

< 의안 소관 부서명 >

국가정보원 국가사이버안보센터	
연 락 처	(02) 2210-8042