



제429회 국회 (정기회)
제14차 행정안전위원회

전자정부법 일부개정법률안

검 토 보 고

〈사이버공격·위협 대응 자체진단·점검 실시〉

■ 김기현의원 대표발의(의안번호 제2212988호)

■ 차지호의원 대표발의(의안번호 제2213017호)

2025. 11.

행 정 안 전 위 원 회

수석전문위원 정순임

목 차

I . 제안경위	1
II . 제안이유 및 주요내용	1
III . 검토의견	3
가. 사이버공격·위협 예방·대응을 위한 자체 진단·점검 및 시정조치 이행에 관한 사항	3
나. 과태료	10
다. ‘사이버공격·위협’의 정의	14

I. 제안경위

[김기현의원 대표발의]

1. 발 의 자 : 김기현의원 등 14인
2. 발의연월일 : 2025. 08. 21.
3. 회부연월일 : 2025. 08. 18.

[차지호의원 대표발의]

1. 발 의 자 : 차지호의원 등 12인
2. 발의연월일 : 2025. 09. 16.
3. 회부연월일 : 2025. 09. 17.

II. 제안이유 및 주요내용

[김기현의원 대표발의]

최근 사이버공격이 잇따라 발생하여 공공기관 등의 사이버보안을 강화해야 할 필요가 강조되고 있음.

그런데 중앙행정기관등의 사이버공격·위협에 대한 예방 및 대응에 필요한 자체 진단·점검 근거는 대통령령인 「사이버안보 업무규정」

에 있어 사이버보안을 실질적으로 강화하기 위하여 진단·점검 의무를 법률로 정하고 시정조치 등도 의무화해야 한다는 지적이 있음.

이에 행정기관등의 장이 해당 기관에 대한 사이버공격·위협의 예방 및 대응에 필요한 자체 진단·점검을 연 1회 이상 실시하고 취약점 등이 발견된 때에는 지체 없이 시정조치 등을 하도록 함(안 제56조 제5항 및 제6항 등).

[차지호의원 대표발의]

2025년 6월 한국연구재단 해킹 사고에서 드러난 바와 같이, 다수 공공기관이 주기적 사이버보안 점검을 내부 지침 수준으로만 운영하여 실효성이 부족하다는 지적이 제기되고 있음.

정보통신망에 대한 해킹·랜섬웨어 공격이 고도화되는 상황에서, 공공기관의 취약점 관리·시정조치를 법률상 의무조항으로 격상하고, 위반 시 과태료를 부과하도록 하여 국민의 개인정보와 국가 주요 연구·기술정보를 보호하려는 것임(안 제56조제5항).

Ⅲ. 검토의견

가. 사이버공격·위협 예방·대응을 위한 자체 진단·점검 및 시정 조치 이행에 관한 사항

개정안들은 행정기관의 장 또는 공공기관의 장에 대하여 사이버공격·위협의 예방 및 대응에 필요한 자체진단·점검 및 시정조치 이행 의무를 규정하려는 것으로,

김기현의원안은 행정기관¹⁾ 및 공공기관²⁾(이하 “행정기관등”)을, 차지호의원안은 공공기관을 대상기관으로 하고 있음.

현행	김기현의원안	차지호의원안
제56조(정보통신망 등의 보안대책 수립·시행) ① ~ ④ (생략) <u><신설></u>	제56조(정보통신망 등의 보안대책 수립· <u>시행</u> 등) ① ~ ④ (현행과 같음) <u>⑤ 행정기관등의 장은 해당 기관에 대한 사이버공격·위협의 예방 및 대응에 필요</u>	제56조(정보통신망 등의 보안대책 수립·시행) ① ~ ④ (현행과 같음) <u>⑤ 공공기관의 장은 매 회계연도 1회 이상 소관 정보통신망 및 정보시스템에 대한 사</u>

1) 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

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.

2) 3. “공공기관”이란 다음 각 목의 기관을 말한다.

가. 「공공기관의 운영에 관한 법률」 제4조에 따른 법인·단체 또는 기관

나. 「지방공기업법」에 따른 지방공사 및 지방공단

다. 특별법에 따라 설립된 특수법인

라. 「초·중등교육법」, 「고등교육법」 및 그 밖의 다른 법률에 따라 설치된 각급 학교

마. 그 밖에 대통령령으로 정하는 법인·단체 또는 기관

현행	김기현의원안	차지호의원안
<신설>	<u>한 자체 진단·점검을 연 1회 이상 실시하여야 한다.</u> ⑥ <u>행정기관등의 장은 제5항의 자체 진단·점검에서 취약점 등이 발견된 때에는 지체 없이 이를 시정하는 등 필요한 조치를 하여야 한다.</u>	<u>이버보안 자체 진단·점검을 실시하고, 취약점이 확인된 경우 확인된 날부터 30일 이내에 시정조치를 완료하여야 한다.</u>

행정안전부에 따르면, 최근 4년간 지자체 대상 해킹 시도 건수는 2021년 10,292건에서 2024년 15,489건으로 증가 추세이고, 2025.8월 기준 8,403건임. 이 중 웹해킹(시스템권한획득, 홈페이지 변조, 정보유출) 분야의 공격이 가장 높아 67.2%를 차지하고, 비인가접근 16.6%, 정보수집 6.9%, 악성코드 5.7% 등임.

[최근 4년간 지자체 대상 사이버공격 유형별 시도 건수]

(단위 : 건)

구분	계	2021	2022	2023	2024	~2025.8.
계	58,018	10,292	10,320	13,514	15,489	8,403
웹해킹 (시스템권한획득)	38,968	8,088	3,261	4,291	4,819	1,686
웹해킹 (홈페이지 변조)			1,378	1,603	1,306	1,322
웹해킹 (정보유출)			2,428	2,730	3,994	2,062
악성코드	3,284	613	718	632	922	399
비인가접근	9,622	975	1,473	2,883	2,691	1,600
서비스거부	2,157	95	75	533	548	906
기타 (정보수집)	3,987	521	987	842	1,209	428

- 주1. 웹해킹은 홈페이지, 웹페이지의 취약점을 이용하여 공격이며 입력값 검증부재, 부적절한 입력·환경설정 등을 통한 웹서버에 대한 악의적인 행위
2. 악성코드는 컴퓨터 바이러스, 웜, 트로이목마, 백도어, 봇, 스파이웨어 등이 사용자의 동의 없이 컴퓨터에 설치되어 사용자의 정보를 탈취하거나 컴퓨터를 오작동 시키고 네트워크를 마비시킬 수 있는 악의적인 행위
3. 비인가접근은 네트워크, 시스템, 응용프로그램, 데이터 또는 기타 자원 등에 인가를 받지 않은 자가 논리적 또는 물리적으로 불법 접근하는 공격 행위
4. 서비스거부는 시스템에 과도한 부하를 유발하여 정상적인 서비스를 차단하거나 성능을 저하시키는 악의적인 행위
5. 기타(정보수집 등)는 서버나 시스템을 공격하기전에 서버 혹은 시스템의 취약점, 네트워크 경로, 방화벽 설치 유무를 알아내고 정보를 수집하는 공격 행위

자료: 행정안전부

최근 한국연구재단 해킹 사건(2025.6월)으로 12만 건의 개인정보 유출,³⁾ 워크넷(현 고용24) 해킹 사건(2023. 6월~7월)으로 23만 건 개인정보 유출,⁴⁾ 법원 해킹 사건(2024.5월)으로 1천여 GB 자료 유출⁵⁾ 등 행정

3) “한국연구재단 해킹으로 개인정보 12만건 털려…개인정보위 조사”, MBC뉴스, 2025.6.13., “개인정보 12만건 털린 한국연구재단 ‘잼스’ 해킹, 예견된 인재”, 뉴스1, 2025.10.24. 등 언론보도 참조

4) “고용부 취업정보사이트 ‘워크넷’ 중국 해커에 뚫렸다…개인정보 23만건 유출”, 뉴스1, 2023.7.6., “정부 구인구직사이트 ‘워크넷’ 23만명 이력서 털렸는데...고용정보원 7일간 몰랐다”, 투데이신문, 2023.10.23. 등 언론보도 참조

기관 및 공공기관의 정보통신망에 대한 해킹 및 랜섬웨어 피해는 계속해서 발생하고 있고, 그 피해도 상당함.

현행 「사이버안보 업무규정」(대통령령) 제12조제1항⁶⁾은 중앙행정기관등(「국가정보원법」 제4조제1항제4호 각 목⁷⁾의 기관)에 대하여 사이버공격·위협의 예방 및 대응에 필요한 자체 진단·점검을 매년 1회 실시하고, 시정조치를 이행하도록 규정하고 있음.

5) “북한, 법원 전산망 해킹해 자료 1천여GB 빼갔다”, KBS뉴스, 2024.5.11., ““北 해킹에 속수무책” 법원행정처, 2억 과징금 철회“, KBS뉴스, 2025.1.9. 등 언론보도 참조

6) 「사이버안보 업무규정」(대통령령) 제12조(사이버보안 자체 진단·점검) ① 중앙행정기관등의 장은 해당 기관에 대한 사이버공격·위협에 대한 예방 및 대응에 필요한 자체 진단·점검을 연 1회 이상 실시해야 한다.

② 제1항에도 불구하고 중앙행정기관등의 장이 다음 각 호의 어느 하나에 해당하는 조치를 한 경우에는 제1항에 따른 자체 진단·점검을 실시한 것으로 본다.

1. 삭제

2. 「정보통신기반 보호법」 제9조에 따른 취약점 분석·평가

3. 제9조제5항에 따른 보안관리 수준 측정

4. 「전자금융거래법」 제21조의3에 따른 전자금융기반시설의 취약점 분석·평가

③ 중앙행정기관등의 장은 제1항에 따른 진단·점검 결과 취약요소가 발견된 경우 이를 시정하는 등 필요한 조치를 해야 한다.

④ 국가정보원장은 사이버공격·위협이 발생하거나 발생할 우려가 있는 중앙행정기관등의 장에게 제1항에 따른 자체 진단·점검 결과 및 제3항에 따른 조치 결과를 제출할 것을 요청할 수 있다. 이 경우 요청을 받은 중앙행정기관등의 장은 정당한 사유가 없으면 그 요청에 따라야 한다.

7) 「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

나. 지방자치단체와 그 소속기관

다. 그 밖에 대통령령으로 정하는 공공기관

「사이버안보 업무규정」 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

개정안들은 「사이버안보 업무규정」(대통령령)에 규정된 사항을 법률로 상향 규정함으로써 행정기관·공공기관의 사이버 보안을 강화하기 위한 취지임.

다만, 개정안과 관련해서는 다음 사항을 고려한 논의가 필요해 보임.

첫째, 개정안들은 「정보통신기반 보호법」 제9조에서 규정하는 사항과 유사한 내용을 지니고 있음.

「정보통신기반 보호법」 제9조제1항8)에서는 주요정보통신기반시설을 관리하는 기관(관리기관)에 대하여 정기적으로 소관 주요정보통신기반시설의 취약점을 분석·평가 의무를, 제2항에서는 중앙행정기관의 장이 새로운 형태의 전자적 침해행위로부터 주요정보통신기반시설을 보호하기 위한 경우, 주요정보통신기반시설에 중대한 변화가 발생하여 별도의 취약점 분석·평가가 필요한 경우 해당 관리기관의 장에게 주요정보통신기

8) 「정보통신기반 보호법」 제9조(취약점의 분석·평가) ① 관리기관의 장은 대통령령으로 정하는 바에 따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석·평가하여야 한다.

② 중앙행정기관의 장은 다음 각 호의 어느 하나에 해당하는 경우 해당 관리기관의 장에게 주요정보통신기반시설의 취약점을 분석·평가하도록 명령할 수 있다.

1. 새로운 형태의 전자적 침해행위로부터 주요정보통신기반시설을 보호하기 위하여 필요한 경우
2. 주요정보통신기반시설에 중대한 변화가 발생하여 별도의 취약점 분석·평가가 필요한 경우
- ③ 관리기관의 장은 제1항 또는 제2항에 따라 취약점을 분석·평가하고자 하는 경우에는 대통령령이 정하는 바에 따라 취약점을 분석·평가하는 전담반을 구성하여야 한다.

제5조(주요정보통신기반시설보호대책의 수립 등) ① 주요정보통신기반시설을 관리하는 기관(이하 "관리기관"이라 한다)의 장은 제9조제1항 또는 제2항에 따른 취약점 분석·평가의 결과에 따라 소관 주요정보통신기반시설 및 관리 정보를 안전하게 보호하기 위한 예방, 백업, 복구 등 물리적·기술적 대책을 포함한 관리대책(이하 "주요정보통신기반시설보호대책"이라 한다)을 수립·시행하여야 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.

반시설의 취약점을 분석·평가를 명할 수 있도록 규정하고 있음.

이처럼 정보시스템 취약점에 대한 분석·평가 관련 내용이 개별법에 중복 규정될 경우 실제 법 집행과정에서 실효성이 저하되고 행정력의 낭비가 우려되는바, 「정보통신기반 보호법」에 따라 취약점 분석·평가를 한 경우 이 법에 따른 자체 진단·점검이 이루어진 것으로 간주 규정을 둘 필요가 있겠음.

둘째, 의무이행 주체와 관련해서 김기현의원안은 ‘행정기관등’, 차지호의원안은 ‘공공기관’으로 규정하고 있는바, 현행법상 보안대책 수립·시행 주체와 「사이버안보 업무규정」(대통령령) 제12조에 따른 자체 진단·점검 및 시행조치 주체 간에 차이가 있는 점을 고려하여 논의가 필요해 보임.

현행법상 보안대책 수립·시행 주체인 행정기관에는 국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관이 해당하나, 「사이버안보 업무규정」(대통령령)에 따라 자체 진단·점검 및 시행조치를 이행하는 중앙행정기관등은 이 기관들을 포함하지 않고 있음.

셋째, 개정안을 수용한다면, 자체 진단·점검의 기준 및 방법, 시행조치의 이행 등에 필요한 사항을 하위법령으로 위임하도록 규정하는 것이 법제적으로 타당해 보임.

자체 진단·점검 및 시행조치 미이행 기관에 대해서는 과태료가 부과 (김기현의원안 제78조제1항제3호·제4호, 차지호의원안 제79조)되는바, 과태료 부과 대상 행위에 해당하는 사항을 명확하게 규정하는 것이 적절함.

참고로, 행정안전부 및 국가정보원은 자체진단 점검결과 취약점이 확인되더라도 시스템 개발, 보안장비 도입 및 예산 수립 절차에 따라 지체 없이(김기현의원안) 또는 30일 이내(차지호의원안) 시정조치가 불가능한 경우가 발생할 수 있으므로, 이 경우 시행조치를 계획하여 이행할 수 있도록 보완할 필요가 있다는 의견을 제시함.

나. 과태료

제56조제5항 및 제6항을 위반한 자에 대하여 김기현의원안은 3천만원 이하의 과태료를, 차지호의원안은 1천만원 이하의 과태료를 부과하도록 규정하려는 것임.

현행	김기현의원안	차지호의원안
제78조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다.	제78조(과태료) ① ---- ----- ----- -----.	
1. 2. (생략) <신설>	1. 2. (현행과 같음) 3. 제56조제5항을 위반하여 자체 진단·점검을 연 1회 이상 실시하지 아니한 자	
<신설>	4. 제56조제6항을 위반하여 취약점 등을 지체 없이 시정하는 등 필요한 조치를 하지 아니한 자	
② (생략) <신설>	② (현행과 같음)	제79조(과태료) ① 제56조제5항을 위반하여 자체 진단·점검을 실시하지 아니하거나

현행	김기현의원안	차지호의원안
<신설>		<u>시정조치를 완료하지 아니한 공공기관의 장에게는 1천만원 이하의 과태료를 부과한다.</u> <u>② 제1항에 따른 과태료 부과·징수 절차 등 필요한 사항은 대통령령으로 정한다.</u>

개정안들은 행정기관 등에 자체 진단·점검 의무 및 시정조치 이행의무 규정의 실효성을 확보하려는 취지로 보임.

다만, 개정안들과 관련해서는 과태료 부과 대상자 및 과태료 한도액의 적정성에 관하여 검토가 필요함.

첫째, 김기현의원안은 과태료 부과 대상에 행정기관을 포함하고 있는바, 현행법상 행정기관의 범위에는 국회·법원·헌법재판소·중앙선거관리위원회가 포함되는 점, 의무 이행사항은 행정기관 간의 협조 등으로 해결될 수 있는 점, 과태료 부과권자(행정안전부장관)와 부과 대상기관(행정안전부)이 같은 점, 유사 입법례 등을 고려한 논의가 필요해 보임.

법제실무상 행정기관 간 협조 등으로 해결이 되지 않을 시 정부조직 내부의 명령체계(국무총리의 조정이나 공무원에 대한 지휘·감독권) 등을 통해 해결할 수 있으므로 신중하게 판단할 필요가 있음.⁹⁾

참고로, 행정기관에 과태료를 부과한 입법례는 「통계법」¹⁰⁾이 있고, 공공기관에 과태료를 부과한 입법례는 「정보통신기반 보호법」¹¹⁾, 「중소기업제품 구매촉진 및 판로지원에 관한 법률」¹²⁾ 등이 있음.

이 중 「정보통신기반 보호법」은 과태료 부과 대상자에서 중앙행정기관을 제외하도록 단서를 두고 있음.

둘째, 과태료의 한도액과 관련해서 김기현의원안은 3천만원 이하, 차지호의원안은 1천만원 이하를 규정하고 있는바, 유사 입법례와의 형평성 등을 고려하여 과태료 한도액 수준을 판단할 필요가 있음.

9) 「법제기준과 실제(2024년

10) 「통계법」 제41조(과태료) ①통계작성기관이 제36조제1항에 따른 시정요구 또는 재발 방지 조치계획 수립 요구(같은 항 제9호의 위반행위로 인한 것으로 한정한다)를 이행하지 아니한 경우에는 500만원 이하의 과태료를 부과한다.

제3조(정의) 3. "통계작성기관"이란 중앙행정기관·지방자치단체 및 제15조에 따라 지정을 받은 통계작성지정기관을 말한다.

11) 「정보통신기반 보호법」 제30조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자에게는 5천만원 이하의 과태료를 부과한다. 다만, 관리기관의 장이 관계중앙행정기관의 장(그 소속기관의 장인 경우를 포함한다)인 경우에는 그러하지 아니하다.

② ~ ⑦ (생략)

12) 「중소기업제품 구매촉진 및 판로지원에 관한 법률」 제37조(과태료) ① 제32조에 따른 자료의 제출 또는 보고를 하지 아니하거나 거짓된 자료를 제출하거나 거짓으로 보고를 한 자 또는 검사를 거부·방해 또는 기피한 자에게는 300만원이하의 과태료를 부과한다.

제32조(보고와 검사 등) ① 중소벤처기업부장관은 이 법을 시행하기 위하여 필요하다고 인정하면 다음 각 호의 어느 하나에 해당하는 자에게 필요한 자료의 제출 및 보고를 요구할 수 있으며, 소속 공무원으로 하여금 해당 사무소와 사업장 등에 출입하여 장부·서류나 사업추진과 관련된 물건을 검사하도록 할 수 있다.

1. 제4조·제5조·제7조·제12조·제31조의2에 따른 공공기관의 장

참고로, 「개인정보 보호법」¹³⁾은 주민등록번호의 암호화 조치를 하지 않은 자에게 3천만원 이하의 과태료, 「정보통신기반 보호법」은 정기적으로 취약점을 분석·평가하지 아니한 자, 취약점 분석·평가 명령에 따르지 아니한 자에게 500만원 이하의 과태료를 규정함.¹⁴⁾

13) 「개인정보 보호법」 제75조(과태료) ② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다.

8. 제24조의2제2항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 암호화 조치를 하지 아니한 자

14) 「정보통신기반 보호법」 제30조(과태료) ③ 다음 각 호의 어느 하나에 해당하는 자에게는 500만원 이하의 과태료를 부과한다. 다만, 관리기관의 장이 관계중앙행정기관의 장(그 소속기관의 장인 경우를 포함한다)인 경우에는 그러하지 아니하다.

1. 제9조제1항을 위반하여 정기적으로 취약점을 분석·평가하지 아니한 자
2. 제9조제2항을 위반하여 취약점 분석·평가 명령에 따르지 아니한 자

다. ‘사이버공격·위협’의 정의

김기현의원안은 ‘사이버공격·위협’이라는 용어를 해킹, 컴퓨터 바이러스, 서비스거부(DDoS: Distributed Denial of Service), 전자기파 등 전자적 수단에 의하여 정보통신기기, 정보통신망 또는 이와 관련된 정보시스템을 침입·교란·마비·파괴하거나 정보를 위조·변조·훼손·절취하는 행위 및 그와 관련된 위협으로 정의하려는 것임(안 제2조제16호 신설).

현행	개정안
제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. 1. ~ 15. (생략) <u><신설></u>	제2조(정의) ----- -----. 1. ~ 15. (현행과 같음) 16. “사이버공격·위협”이란 해킹, 컴퓨터 바이러스, 서비스거부(DDoS: Distributed Denial of Service), 전자기파 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.

개정안은 ‘사이버공격·위협’이라는 용어를 명확하게 정함으로써 관련 규정의 해석상의 혼란을 방지하기 위한 취지로 보임.

다만, 정의하려는 용어가 법률 전반에 걸쳐 사용되지 않는 경우 해당 조항에서 그 의미를 규정하는 것이 적절하다는 점에서, ‘사이버공격·위협’이라는 용어는 안 제56조제5항에서만 사용되고 있으므로 이를 정의규정에 두기보다 안 제56조제5항에 두는 방식이 적절함.

참고로, ‘사이버공격·위협’이라는 용어를 정의한 유사 입법례는 없는 것으로 파악됨.

문 의 처
02)6788-5339