



COUNTRY: GREECE

Greece does not have a cybersecurity strategy or dedicated cybersecurity legislation. The legal and institutional framework that supports cybersecurity is also limited. The national computer emergency response team, NCERT-GR, is limited to government institutions and operators of critical infrastructure.

There are no significant public-private partnerships in Greece, and the government is not actively pursuing their establishment or closer cooperation with the private sector.

QUESTION	RESPONSE	EXPLANATORY TEXT
LEGAL FOUNDATIONS		
1. Is there a national cybersecurity strategy in place?	No	According to the European Union Agency for Network and Information Security (ENISA) < www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategy-3 >, Greece is in the process of preparing a cybersecurity strategy.
2. What year was the national cybersecurity strategy adopted?	–	
3. Is there a critical infrastructure protection (CIP) strategy or plan in place?	✓	Presidential Decree 39/2011 Regarding Critical Infrastructure Protection harmonises Greek legislation with the European Union Directive 2008/114/EC on the identification, designation, and assessment of critical infrastructure. In addition, the Regulation for the Safety and Integrity Network and Electronic Communications Services 2013 < www.adae.gr/fileadmin/docs/enimerosi/sxedio_kanonismou_adae_asfaleia_akeraiotita.pdf > addresses network-based and electronic critical infrastructure.
4. Is there legislation/policy that requires the establishment of a written information security plan?	🕒	While there is no legislation or policy in place in Greece that requires the establishment of a written information security plan, the Assurance Authority for Confidentiality of Communication (ADAE) < www.adae.gr > has published the Regulation for the Safety and Integrity Network and Electronic Communications Services.
5. Is there legislation/policy that requires an inventory of “systems” and the classification of data?	✓	Law 3649/2008 on the National Intelligence Service grants responsibility for the classification of government data to the National Intelligence Service (NIS). < www.nis.gr > The NIS carries out classification according to a four-tiered system of classification. There is neither a legislative requirement for specific data to be classified nor a requirement to develop a particular inventory of classification systems.
6. Is there legislation/policy that requires security practices/requirements to be mapped to risk levels?	✗	There is no legislation or policy in place in Greece that requires security practices/requirements to be mapped to risk levels.
7. Is there legislation/policy that requires (at least) an annual cybersecurity audit?	✗	There is no legislation or policy in place in Greece that requires an annual cybersecurity audit.
8. Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	✗	There is no legislation or policy in place in Greece that requires a public report on cybersecurity capacity for the government.
9. Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	✗	There is no legislation or policy in place in Greece that requires a chief information officer or chief security officer.
10. Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✗	Reporting is advised in the general measures issued to government agencies by NCERT-GR. < www.nis.gr/portal/page/portal/NIS/NCERT > However there is no legislation or policy in place that requires reporting to be mandatory.

COUNTRY: GREECE

QUESTION	RESPONSE	EXPLANATORY TEXT
11. Does legislation/policy include an appropriate definition for “critical infrastructure protection” (CIP)?	✓	Presidential Decree 39/2011 Regarding Critical Infrastructure Protection adopts the European Union Directive 2008/114/EC’s definition for “critical infrastructure protection”.
12. Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	✓	The Regulation for the Safety and Integrity Network and Electronic Communications Services 2013 <www.adae.gr/fileadmin/docs/enimerosi/sxedio_kanonismou_adae_asfaleia_akeraiotita.pdf> specifically references EU and international standards for security certification and accreditation. It covers all ICT systems, critical infrastructure, and network and electronic communication services in Greece.
OPERATIONAL ENTITIES		
1. Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✓	NCERT-GR <www.nis.gr/portal/page/portal/NIS/NCERT> was established in 2009. It is responsible for coordinating incident response measures for both government institutions and entities engaged with critical public infrastructure.
2. What year was the computer emergency response team (CERT) established?	2009	
3. Is there a national competent authority for network and information security (NIS)?	✓	<p>The Assurance Authority for Confidentiality of Communication (ADAE) <www.adae.gr> acts as the primary body responsible for network and information security in Greece.</p> <p>The National Intelligence Service of Greece (NIS) <www.nis.gr> handles matters related to information and network security as outlined in Law 3649/2008. <www.nis.gr/npimages/docs/LAW_NUMBER%203649_en.pdf> These duties include the administration of NCERT-GR, the national CERT. There is not, however, a body or agency within the NIS dedicated to network and information security — apart from the limited, response-focused scope of NCERT-GR.</p> <p>The Directorate of Cyber Defence, reporting to the Chief of Defence is responsible for cyber warfare and liaises with the NIS and the Greek police services.</p> <p>The Greek Cybercrime Centre <www.cybercc.gr> is a national project aimed primarily at improving research and education in the area of cyber attacks. It does not handle network and information security at large.</p>
4. Is there an incident reporting platform for collecting cybersecurity incident data?	✓	NCERT-GR <www.nis.gr/portal/page/portal/NIS/NCERT> is responsible for the collection of cybersecurity incident data. It maintains an emailed-based reporting platform to log cybersecurity incidents.
5. Are national cybersecurity exercises conducted?	✓	Greece conducted the national cybersecurity exercise Panoptis four times in the period 2010 to 2014.
6. Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✗	The Measures for the Protection of Information Systems Against Cyber Attacks contains the minimum standards for government information systems, which includes provision for incident detection and reporting, but does not include an incident management structure.
PUBLIC-PRIVATE PARTNERSHIPS		
1. Is there a defined public-private partnership for cybersecurity?	✗	There is no defined public-partnership for cybersecurity in Greece.
2. Is industry organised (i.e. business or industry cybersecurity councils)?	✗	There is no significant industry-led platform for cybersecurity in Greece.
3. Are new public-private partnerships in planning or underway (if so, which focus area)?	✗	There are no new public-private partnerships being planned in Greece.
SECTOR-SPECIFIC CYBERSECURITY PLANS		
1. Is there a joint public-private sector plan that addresses cybersecurity?	✗	Greece does not have sector-specific joint public-private plans in place.
2. Have sector-specific security priorities been defined?	✗	Sector-specific security priorities have not been defined.
3. Have any sector-specific cybersecurity risk assessments been conducted?	✗	Sector-specific risk assessments have not been released.



COUNTRY: GREECE

QUESTION	RESPONSE	EXPLANATORY TEXT
EDUCATION		
1. Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	✘	Greece is preparing a national cybersecurity strategy and this may contain education commitments. Additionally, the Greek Cybercrime Centre < www.cybercc.gr/en > plays a limited role in promoting educational activities in the cybersecurity field.