

>>Information Assurance

Frequently Asked Questions

1. [What is Information Assurance?](#)
 2. [How has the Information Assurance mission evolved?](#)
 3. [What are the five Information Assurance pillars?](#)
 4. [How are the five pillars of Information Assurance applied?](#)
 5. [Is there a national Information Assurance strategy?](#)
 6. [What is Defense-In-Depth?](#)
-

1. What is Information Assurance?

Information Assurance is defined as the set of measures intended to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. These measures are planned and executed by the Information Assurance Directorate (IAD) of the National Security Agency/Central Security Service (NSA/CSS).

[Return to the Top](#)

2. How has the Information Assurance mission evolved?

The mission has evolved through three very distinct stages: Communications Security (COMSEC), Information Systems Security (INFOSEC) and Information Assurance (IA). Post WWI and the Korean War, COMSEC efforts focused primarily on cryptography (i.e., designing and building encryption devices to provide confidentiality for information). The introduction and widespread use of computers created new demands to protect information exchanges between interconnected computer systems. This demand created the Computer Security (COMPUSEC) discipline. With the introduction of COMPUSEC came the recognition that stand-alone COMSEC and stand-alone COMPUSEC could not protect information during storage, processing or transfer between systems. This recognition gave rise to the term INFOSEC and the information protection mission took on a broader perspective. IA emerged and focused on the need to protect information during transit, processing, or storage within complex and/or widely dispersed computers and communication system networks. IA includes a dynamic dimension where the network architecture is itself a changing environment, including the information protection mechanisms that detect attacks and enable a response to those attacks.

[Return to the Top](#)

3. What are the five Information Assurance pillars?

The five information assurance (IA) pillars are availability, integrity, authentication, confidentiality, and non-repudiation. These pillars and any measures taken to protect and defend information and information systems, to include providing for the restoration of information systems, constitute the essential underpinnings for ensuring trust and integrity in information systems.

The cryptologic components of information assurance primarily address the last four pillars of integrity, authentication, confidentiality, and non-repudiation. These pillars are applied in accordance with the mission needs of particular organizations.

[Return to the Top](#)

4. How are the five pillars of Information Assurance applied?

How the five pillars are applied is determined by the sensitivity of the information or information system, the threat, and other risk management decisions. These pillars are the heart of the U.S. Government's ability to conduct secure operations in a globally networked environment.

[Return to the Top](#)

5. Is there a national Information Assurance strategy?

In moving information assurance (IA) forward to protect the National Information Infrastructure (NII), a National Information Assurance Strategy (NIAS) was formed to encourage mutual cooperation and acceptance of common objectives. This strategy, built upon the following five cornerstones, articulated the IA pillar concepts into a national framework that unified the U.S. Government's IA efforts:

- Cyber security awareness and education;
- Strong cryptography;
- Good security-enabled commercial information technology;
- An enabling global Security Management Infrastructure; and
- A civil defense infrastructure equipped with an attack sensing and warning capability and coordinated response mechanisms.

[Return to the Top](#)

6. What is Defense-In-Depth?

Defense-In-Depth strategy integrates People, Operations, and Technology capabilities to establish information assurance (IA) protection across multiple layers and dimensions. Successive layers of defense will cause an adversary who penetrates or breaks down one barrier to promptly encounter another Defense-In-Depth barrier, and then another, until the attack ends.

[Return to the Top](#)