How can a small business handle all the requirements that the Department of Defense imposes?
Build and Operate a Trusted GIG

CIAA GAC-1: ORGANIZE

1.1 Lead and Govern

1.2 Design for the Fight

1.3 Develop the Workforce

2.1 Secure Data in Transit

2.2 Manage Access

2.3 Assure Information Sharing

3.1 Understand the Battlespace

3.2 Prevent and Delay Attackers...

3.3 Prevent Attackers from Staying...

4.1 Develop and Maintain Trust...

4.2 Strengthen Cyber Readiness

4.3 Sustain Missions

SUBORDINATE POLICY

Cyber, Identity & Information Assurance (CIAA) Related Policies and Issuances

NATIONAL / FEDERAL

AUTHORITIES

DISTRICT

ABOUT THIS CHART

This chart organizes information assurance policies and guidance by CIAA Strategic Goal and Office of Primary Responsibility (specify OPR). It is intended to show all IC-related policies. A component may need to comply with and direct users to the full text. This chart is meant to link to the most authoritative source for each document. We check the integrity of the links on a regular basis, but have no control over the sites linked to, so you may occasionally experience an error message due to problems at the source site or the site's decision to move the document. Please let us know if you believe the link is no longer valid.

No priority is defined by the arrangement of the guidance boxes. In the electronic version, each policy and the OPN in the Color Key are hyperlinked to their full text or respective sites online. To use the hyperlink, simply click on the box. Policies in italics indicate the document is marked for limited distribution or is not public-facing. Hyperlink is currently available.

Beware with red borders were updated since 28 September 2010. For printing, this chart is best viewed on 22"x27" (Size C) paper. Note: Users of the iPad, iPhone or iPod Touch may find they can view this chart but that its interactive elements are inoperable, because of Apple's restriction on not fully support certain Adobe products. For those who desire a workaround for this issue, there are apps on the iTunes store for less than $0.99.

For the latest version of this chart go to http://dis.os.dla.mil/attacols/glossary/chart.html

Partnet and DOD EMall
How can a small company keep up with so many security requirements?

- DOD Security Technical Implementation Guidelines STIGs
  - Application Security and Development
  - Operating Systems
  - Web servers
  - Application servers
  - Networking
- PCI-DSS
1. Everyone Owns Security

• We consider ourselves a security company
• Out of about 40 employees:
  – Half have security training
  – 5 are directly responsible
• Security isn't something that someone else does
• All Developers know OWASP Top Ten
  – Code Review each other
2. Tools and Open Source

- Establish common frameworks
- Open Source
  - OWASP Tools
- Build our own
- Scanning Tools
3. Discipline

- Small Company = Flexibility
- Small Company ≠ Undisciplined
- Process, CMMI ≠ Shackles
- Process = Freedom to do what we say we will do.
- Build a solid process with security habits
  - OWASP SAMM or BSIMM as a guide
- DoD: Work with IA Officer and Branch
  - Seek clarity of which requirements apply