

Department of Defense Directive 8100.2 Compliance Report

Designated Official: _____

Time Period: 09:50:15 Thursday, July 07, 2005

What is the DoD Directive Number 8100.2?

The Department of Defense (DoD) Directive Number 8100.2 (the Directive hereafter) stipulates the key policy sections regarding the use of commercial wireless devices, services, and technologies in the DoD. Its purpose is to safeguard the DoD networks from the security vulnerabilities inherent with wireless networks, making security a prerequisite for the deployment and use of commercial wireless technologies in the DoD.

Why is the Directive so important?

Wireless networks are more vulnerable to external attacks than wired ones. This is especially true for the 802.11 network. Radio signals extend beyond the boundaries of buildings, leaving the network wide open to hackers; as a shared network, a loophole in any part of the network can expose the entire WLAN to external attacks; and with the rapid adoption of the 802.11 network comes an ever-increasing number of sophisticated tools that hackers use to break the encryption and authentication techniques used for network access. Therefore, the DoD Directive Number 8100.2 is a step in the right direction for safeguarding DoD wireless networks.

What is the scope of the Directive?

The Directive is geared towards securing all commercial wireless devices, services, and technologies for non-classified information, be it data or voice. It explicitly prohibits the use of wireless devices for transmission, storage, or processing of classified information. The commercial wireless devices include wireless-enabled computer systems, PDAs, mobile phones, handheld scanners, 802.11 wireless networks, etc.

To whom does the Directive apply?

The Directive applies to personnel in all DoD organizations, including DoD contractors, visitors of DoD facilities, and anyone who has access to DoD information.

How will the Directive affect 802.11 networks?

Many of the policies spelt out in the Directive are applicable to the 802.11 wireless technologies used in DoD entities. The key policy sections that are relevant to the 802.11 networks include the implementation and enforcement of no 802.11 use in designated areas deemed too risky for the use of wireless technologies; requirement of strong authentication and encryption for network access; mitigation of denial of service and other disruptive attacks; implementation of mechanisms to assess the risks and vulnerabilities associated with 802.11 networks and devices; development of defensive measures to detect, deter, and defeat unauthorized 802.11 activities; integration of intrusion detection methodologies with 802.11 wireless network systems;

AirMagnet DoD Compliance Reports

Policies will be useless without an effective mechanism to monitor and enforce their compliance. AirMagnet automates the monitoring of your wireless networks and devices in compliance with the Directive. The compliance reports integrate the Directive with AirMagnet's advanced IDS/IPS system to provide superior protection for all wireless networks and devices. The reports refer to specific policy sections of the Directive and show the status of compliance of your WLAN. The integrated AirMagnet IDS/IPS algorithms pinpoint the exact cause of violation should it ever occur so that actions can be taken right away to mitigate and/or resolve the problem.



1/ System Level Compliance Report

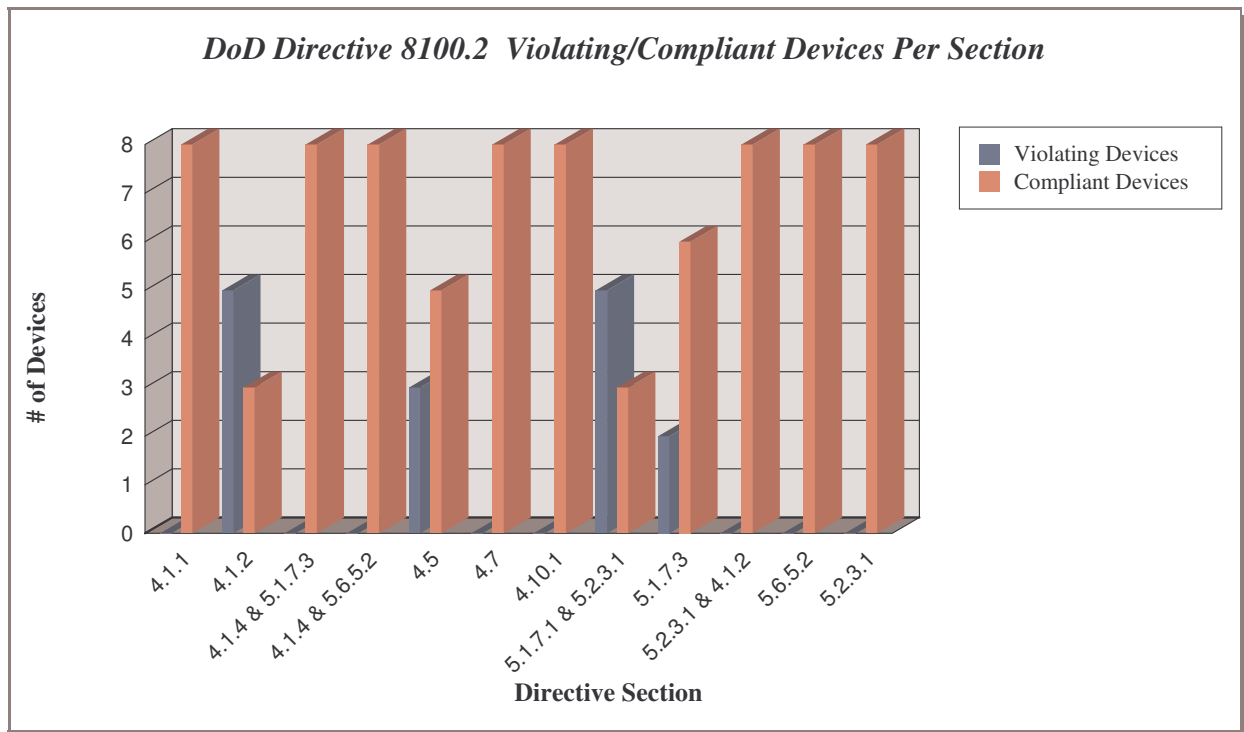
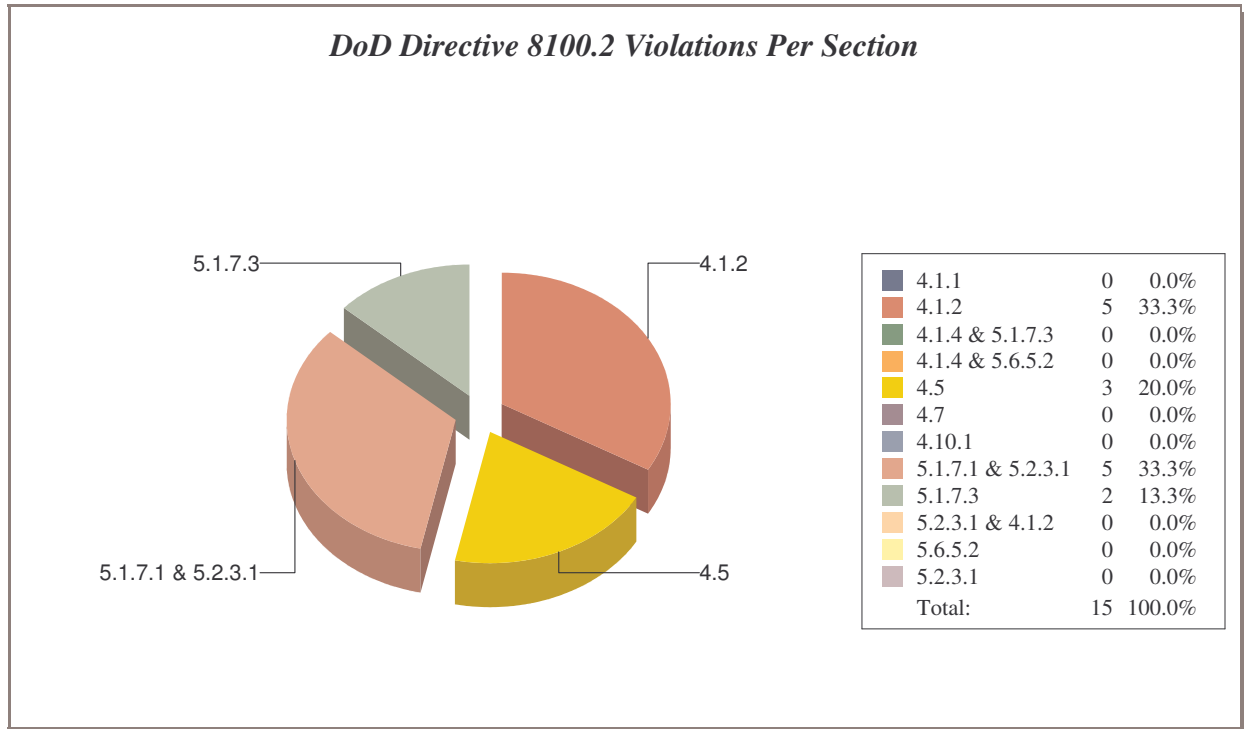
This report summarizes your network's overall compliance with the DoD Directive on a per-policy basis.

DoD Directive 8100.2 Policy Sections	Compliance %
4.10. A DoD wireless KM process shall be established. The goal is increased sharing of DoD wireless expertise to include information on vulnerability assessments, best practices, and procedures for wireless device configurations and connections.	100%
4.10.2. DAAs shall submit alternative mitigating techniques for inclusion in the KM database. The DoD Components shall use the KM process to coordinate, prioritize, and avoid duplication of vulnerability assessments of wireless devices.	100%
5.1.1. Monitor and provide oversight and policy development of all DoD wireless activities.	100%
5.1.4. Direct the development of acquisition strategies and assess potential architectures (e.g., wireless application frameworks) to minimize costs of wireless development, services and systems, achieve economies of scale, and promote interoperability and security. As necessary, coordinate these activities with the Under Secretary of Defense for Acquisition, Technology, and Logistics.	100%
5.2.3.3. Serve as the DoD focal point for IA wireless technologies research and development in support of IA requirements to include protection mechanisms, detection and monitoring, response and recovery, and IA assessment tools and techniques.	100%
5.6.1. Submit to the DoD CIO, within 180 days of this Directive, specific implementation timelines for compliance of legacy systems to this Directive.	100%



2/ Policy Level Compliance Report

This report summarizes your network's compliance on a per-policy basis, showing you the total number of devices that are in compliance or violation of each and every policy in the DoD Directive. By default, your network fails the compliance if one of the devices is in violation of the policy.



<u>DoD Directive 8100.2 Policy Sections</u>	Policy Violation	# Violating Devices	# Compliance Devices	Compliance %
4.1.1: For data, strong authentication, non-repudiation, and personal identification are required for access to a DoD IS in accordance with published DoD policy and procedures. Identification and Authentication (I&A) measures shall be implemented at both the device and network level. I&A of unclassified voice is desirable; voice packets across an Internet protocol (e.g., Voice over Internet Protocol (VoIP)) shall implement I&A in accordance with published DoD policy and procedures.	0	0	8	100.00%
4.1.2: Encryption of unclassified data for transmission to and from wireless devices is required. Exceptions may be granted on a case-by-case basis as determined by the Designated Approving Authority (DAA) for the wireless connections under their control. At a minimum, data encryption must be implemented end-to-end over an assured channel and shall be validated under the Cryptographic Module Validation Program as meeting requirements per Federal Information Processing Standards (FIPS) Publication (PUB) 140-2, Overall Level 1 or Level 2, as dictated by the sensitivity of the data (reference (g)).	5	5	3	37.50%
4.1.4: Measures shall be taken to mitigate denial of service attacks. These measures shall address not only external threats, but potential interference from friendly sources. 5.1.7.3: Provide interoperability testing for wireless devices and operational support for spectrum deconfliction and interference resolution.	0	0	8	100.00%
4.1.4: Measures shall be taken to mitigate denial of service attacks. These measures shall address not only external threats, but potential interference from friendly sources. 5.6.5.2: Include intrusion detection methodologies for the wireless systems.	0	0	8	100.00%
4.5: The DoD Components shall actively screen for wireless devices. Active electromagnetic sensing at the DoD or contractor premises to detect/prevent unauthorized access of DoD ISs shall be periodically performed by the cognizant DAA or Defense Security Service office to ensure compliance with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) ongoing accreditation agreement (reference (f)).	3	3	5	62.50%
4.7: PEDs that are connected directly to a DoD-wired network (e.g., via a hot synch connection to a workstation) shall not be permitted to operate wirelessly while directly connected.	0	0	8	100.00%
4.10.1: The KM process shall be utilized by DAAs to help determine acceptable uses of wireless devices and employ appropriate mitigating actions.	0	0	8	100.00%
5.1.7.1: Incorporate wireless considerations in its DoD-wide Information Assurance (IA) initiatives such as computer emergency response, vulnerability alerting, and enterprise anti-virus and file/data store encryption software. 5.2.3.1: Implement a capability to assess the risks and vulnerabilities associated with wireless technologies that are responsive to DoD requirements.	5	5	3	37.50%
5.1.7.3: Provide interoperability testing for wireless devices and operational support for spectrum deconfliction and interference resolution.	2	2	6	75.00%



5.2.3.1: Implement a capability to assess the risks and vulnerabilities associated with wireless technologies that are responsive to DoD requirements. 4.1.2: Encryption of unclassified data for transmission to and from wireless devices is required. Exceptions may be granted on a case-by-case basis as determined by the Designated Approving Authority (DAA) for the wireless connections under their control. At a minimum, data encryption must be implemented end-to-end over an assured channel and shall be validated under the Cryptographic Module Validation Program as meeting requirements per Federal Information Processing Standards (FIPS) Publication (PUB) 140-2, Overall Level 1 or Level 2, as dictated by the sensitivity of the data (reference (g)).	0	0	8	100.00%
5.6.5.2: Include intrusion detection methodologies for the wireless systems.	0	0	8	100.00%
5.2.3.1. Implement a capability to assess the risks and vulnerabilities associated with wireless technologies that are responsive to DoD requirements.	0	0	8	100.00%

DoD Directive 8100.2 Policies			
AirMagnet Alarms	# Violating Devices	# Compliance Devices	Compliance %
4.1.2: Encryption of unclassified data for transmission to and from wireless devices is required. Exceptions may be granted on a case-by-case basis as determined by the Designated Approving Authority (DAA) for the wireless connections under their control. At a minimum, data encryption must be implemented end-to-end over an assured channel and shall be validated under the Cryptographic Module Validation Program as meeting requirements per Federal Information Processing Standards (FIPS) Publication (PUB) 140-2, Overall Level 1 or Level 2, as dictated by the sensitivity of the data (reference (g)).			
Device unprotected by TKIP	1	7	87.50%
AP with encryption disabled	3	5	62.50%
WEP IV key reused	1	7	87.50%
4.5: The DoD Components shall actively screen for wireless devices. Active electromagnetic sensing at the DoD or contractor premises to detect/prevent unauthorized access of DoD ISs shall be periodically performed by the cognizant DAA or Defense Security Service office to ensure compliance with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) ongoing accreditation agreement (reference (f)).			
Rogue AP by MAC address (ACL)	3	5	62.50%
5.1.7.1: Incorporate wireless considerations in its DoD-wide Information Assurance (IA) initiatives such as computer emergency response, vulnerability alerting, and enterprise anti-virus and file/data store encryption software. 5.2.3.1: Implement a capability to assess the risks and vulnerabilities associated with wireless technologies that are responsive to DoD requirements.			
AP broadcasting SSID	5	3	37.50%
5.1.7.3: Provide interoperability testing for wireless devices and operational support for spectrum deconfliction and interference resolution.			
Excessive missed AP beacons	1	7	87.50%
Excessive low speed transmission	1	7	87.50%

Notes:

- 1) By default, your network fails to comply with the Department of Defense (DoD) Directive 8100.2 if one of the devices violates any of its policy sections.
- 2) Channel specific policy violations will not be included in the Device-Specific Compliance Report.



3/ Device-Specific Compliance Report

This report contains detailed information about devices in compliance or violation of the DoD Directive. It checks the devices against each and every provision in the Directive to show what policy sections are violated or upheld to. It lists all wireless devices deployed on your WLAN. The devices can be sort by MAC address, media type, SSID, or vendor.

Device Information	DoD Directive 8100.2 Policy Sections												Compliance %
	4.1.1	4.1.2	4.1.4 & 5.1.7.3	4.1.4 & 5.6.5.2	4.5	4.7	4.10.1	5.1.7.1 & 5.2.3.1	5.1.7.3	5.2.3.1 & 4.1.2	5.6.5.2	5.2.3.1	
00:02:6F:20:B3:F7-a Channel: 56 5354a	P	P	P	P	F	P	P	F	F	P	P	P	75.00%
00:02:6F:04:88:6A-b Channel: 1 1d2d70	P	F	P	P	P	P	P	P	P	P	P	P	91.67%
00:0F:66:42:D2:B5-b Channel: 11 kassandra	P	F	P	P	P	P	P	F	P	P	P	P	83.33%
00:02:6F:09:3E:2B-b Channel: 1 1d2d70	P	F	P	P	P	P	P	F	P	P	P	P	83.33%
00:02:6F:20:B3:F8-b Channel: 11 5354g	P	F	P	P	F	P	P	F	P	P	P	P	75.00%
00:02:6F:34:A1:59-b Channel: 6 3054g	P	F	P	P	F	P	P	F	P	P	P	P	75.00%

