



# Goddard Procedures and Guidelines

DIRECTIVE NO. GPG 2810.2 APPROVED BY Signature: Original Signed by  
EFFECTIVE DATE: July 9, 2004 NAME: A. V. Diaz  
EXPIRATION DATE: July 9, 2009 TITLE: Director

---

---

**Responsible Office:** 290/Information Services Division

**Title:** Wireless Networks and Access Points

---

## PREFACE

### P.1 PURPOSE

This directive provides direction to ensure that the integrity, availability, and confidentiality of wired networks that interface with, or are accessible by, wireless networks and wireless access points on the National Aeronautics and Space Administration (NASA) Goddard Space Flight Center (GSFC) are safeguarded.

### P.2 APPLICABILITY

a. This directive applies to all GSFC employees and contracts (as provided by the terms and conditions of the contract) where appropriate in achieving Center missions, programs, projects, and institutional requirements. GSFC includes the Wallops Flight Facility, Goddard Institute for Space Studies, and the Independent Verification and Validation Facility.

b. This directive applies to all wireless data communication devices that provide an access point to any wired or Wireless Local Area Network (WLAN) on GSFC. Included are 802.11, Bluetooth, and any other wireless technology configured to enable access to any GSFC wireless (or wired) Local Area Network (LAN). Specifically excluded are wireless clients. Devices such as laptops equipped with a wireless Ethernet card, wireless Personal Digital Assistants, and Internet capable cell phones shall be treated the same as remote user access and are covered under the [GSFC policy governing remote access](#).

### P.3 AUTHORITY

- a. [NPD 2810.1](#), Security of Information Technology
- b. NASA Information Technology Guidelines, [NITG-2810-1](#), Wireless Guidelines

### P.4 REFERENCES

- a. [Dialup Networking – Goddard Connect](#)
- b. [NPR 2810.1](#), *Security of Information Technology*
- c. [NPR 1620.1](#), *Security Procedures and Guidelines*
- d. National Telecommunications and Information Administration, [Technical Standards for Federal Non-Licensed Devices](#)
- e. [NASA-STD-2813](#), *NASA Firewall Strategy, Architecture, Standards and Products*

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT  
<http://gdms.gsfc.nasa.gov/gdms> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

**DIRECTIVE NO.** GPG 2810.2  
**EFFECTIVE DATE:** July 9, 2004  
**EXPIRATION DATE:** July 9, 2009

- f. Title 47 of the Code of Federal Regulations (CFR), Part 5, [Federal Communications Commission \(FCC\)](#)
- g. Title 47 of the Code of Federal Regulations, Part 15, [Radio Communication Devices](#)
- h. National Institute of Standards and Technology (NIST) Special Publication 800-48, [Wireless Network Security – 802.11, Bluetooth and Handheld Devices](#)

**P.5 CANCELLATION**

None

**P.6 SAFETY**

None

**P.7 TRAINING**

Vendor-provided user training will be provided for the Center Network Environment (CNE) Network Operations Center and maintenance staff as part of the GSFC Wireless CNE (WCNE) provisioning contract.

**P.8 RECORDS**

Record Title	Record Custodian	Retention
Account Request Document	Center Information Technology (IT) Security Manager	*NRRS 2/12B2: Destroy when 8 years old.
Completed Configuration Change/Approval Requests	Code 291	*NRRS 8/9A&B: Retire to Federal Records Center (FRC) when 2 years old. Destroy when 30 years old. Earlier destruction is authorized upon receipt of specific authorization from pertinent Center Director or Program Manager.
Inspection Report – Compliance of Pre-existing Wireless Access Points	Code 291	*NRRS 8/9A&B: Retire to FRC when 2 years old. Destroy when 30 years old. Earlier destruction is authorized upon receipt of specific authorization from pertinent Center Director or Program Manager.

\* NASA Records Retention Schedules ([NPR 1441.1](#))

**P.9 METRICS**

- a. Total number of pre-existing wireless access points
  - (1) Number in compliance at the start
  - (2) Number not in compliance at the start
  - (3) Number not in compliance at the end of each subsequent quarter

- b. Total number of new wireless access points to be provided under WCNE
- (1) Number installed and operational at the end of each quarter starting with Installation Start Date
  - (2) Number projected to be installed during the next quarter
  - (3) Difference: number projected to be installed minus the number actually installed [A negative number indicates being ahead of schedule, e.g., 12 (scheduled) - 16 (installed) = -4 or 4 more than scheduled.]

## **P.10 DEFINITIONS**

- a. Non-licensed device - one allowed by Part 15 of the FCC Rules and Regulations ([47 CFR 15](#)). A product in almost any frequency band that meets "low power" requirements, "will not interfere with any properly licensed device", and "accepts any interference from any authorized radio system or other non-licensed device." Such devices shall "bear this statement of limitations to operations."
- b. Physical Security – a state arising from the application of one or more measures such as room and facility access controls, identification of personnel, and protection of the external boundary. Personnel identification may be via measures such as photo ID, biometric devices, or card badge readers. Room and facility access may be controlled by such methods as cipher locks, keypads, and proximity card badge readers. External boundary protection may be supported through use of techniques such as video cameras and locked doors.
- c. Server Set ID (SSID) - a configurable identification that allows clients to communicate to the appropriate base station. With proper configuration, only clients that are configured with the same SSID can communicate with base stations having the same SSID. SSID, from a security point of view, acts as a simple single shared password between base stations and clients.
- d. Wired Equivalency Privacy - a security protocol for wireless local area networks defined in the 802.11b standard. Wired Equivalency Privacy (WEP) is designed to provide the same level of security as that of a wired LAN. LANs are inherently more secure than WLANs because LANs are somewhat protected by the physical nature of their connections, having some or all parts of the network inside a building that can be protected from unauthorized access. WLANs, which are over radio waves, do not have the same physical structure and therefore are more vulnerable to tampering. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not as secure as once believed. WEP is used at the two lowest layers of the Open System Interconnection the data link and physical layers; it therefore does not offer end-to-end security.
- e. Wireless - a method of transferring information from one physical device to another without use of a physical connection between those devices, e.g., by use of radio frequency transmission.
- f. Wireless access point - a device which allows use of wireless networking interfaces in computers and other electronic devices to communicate with a wired network. A wireless access point typically consists of an Ethernet port, radio communications, and sometimes a modem.

## P.11 ABBREVIATIONS AND ACRONYMS

CCB	Configuration Control Board
CIO	Chief Information Officer
CIT	Customer Interface Team
C-ITSM	Center Information Technology Security Manager
CNE	Center Network Environment
CSM	Customer Service Manager
FCC	Federal Communications Commission
FRC	Federal Records Center
GPG	Goddard Procedures and Guidelines
GSFC	Goddard Space Flight Center
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NITG	NASA Information Technology Guidelines
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
NRRS	NASA Records Retention Schedules
SSID	Server Set Identification
STD	Standard
WCNE	Wireless Center Network Environment
WEP	Wired Equivalency Privacy
WLAN	Wireless Local Area Network

## PROCEDURES

GSFC WLAN resources will be treated as network infrastructure and thus must follow all existing security and network standards, procedural requirements [e.g. [NPR 2810.1](#) and any interim guidance issued by the Headquarters NASA and GSFC Chief Information Officers (CIO)]. Wireless networks and/or wireless access points are prohibited on GSFC's CNE ([NASA STD-2813](#)). Wireless networks and wireless access points are prohibited on NASA mission critical networks, e.g., Internet Protocol (IP) Operational Network. Pre-existing wireless networks and wireless access points must be compliant with NASA and GSFC wireless policy and security requirements or be disconnected. No "grandfathering" will be offered or allowed for pre-existing but non-complying wireless networks and wireless access points. However, owners of pre-existing wireless networks and wireless access points will be provided written notice by the Center Information Technology Security Manager (C-ITSM) that they have six months in which to bring non-compliant systems into compliance. If, after these six months have passed, the systems remain non-compliant, the C-ITSM will direct in writing that the non-compliant systems be deactivated with seizure by the C-ITSM of listed/named equipment being an option.

## 1. User Authentication and Authorization

1.1 Access to wireless network connectivity shall be limited to authenticated users and approved wireless devices which are authorized by the GSFC Code 290 Configuration Control Board (CCB).

1.2 Authentication shall be performed using a Virtual Private Network (VPN) or Code 297 approved encryption protocols to ensure confidentiality of authenticating information. Other authentication approaches may be used if and only if they are approved by the GSFC Code 290 CCB. NIST [Special Publication 800-48](#) best practices shall be followed.

1.3 Wireless user accounts shall not be shared. The user authentication methods employed must provide individual accountability for each user accessing GSFC WLAN resources. Once authorized access (user authentication) is gained through GSFC WLAN resources, existing authorization methods will be used to gain access to computing resources on GSFC wired LANs as if the user were on the GSFC wired LAN.

1.4 Strong authentication (e.g., VPN or 802.1X mutual authentication protocols such as Extensible Authentication Protocol and Protected Extensible Authentication Protocol) shall be implemented where feasible.

1.5 The only design architecture permitted for GSFC WLANs is an infrastructure network that provides for an association between a specific access point and a connection to the wired LAN. *Ad hoc* networks (i.e., anonymous, peer, or peer/institutional clients) are prohibited.

1.6 Access points shall be established only on an approved GSFC registered IP address or Reserved Internet space.

1.7 Code 297 shall conduct periodic monitoring of GSFC WLANs for compliance with the provisions of the GPG.

## 2. Wireless Data Confidentiality

2.1 Wireless transmissions of Mission and Business and Restricted Technology data as well as material marked "Administratively Controlled Information" are prohibited unless the wireless network's transmission is performed using Code 297 approved encryption protocols which include, but are not limited to, Secure Sockets Layer, Secure Shell (Version 2), and IPsec.

2.2 WEP and Server Set Identification (SSID), static WEP keys and SSID, and Media Access Control address filtering shall not be employed as the only security measures.

2.3 All wireless transmissions into a GSFC LAN must use a Code 297 approved encryption method. WLAN access points shall utilize dynamic link encryption that is unique for each user and session.

### 3. WLAN Availability

**3.1** WLANs and wireless access points must be confined to (a) logically isolated networks, (b) physically isolated networks, or (c) connected to a GSFC Open network (as defined in NASA-STD-2813). Waivers may be requested from Code 297 and granted on a case-by-case basis. A security assessment and impact report shall be prepared by Code 297 for each waiver granted.

**3.2** WLANs and wireless access points are prohibited for use where availability is a critical performance parameter of the service or interface.

### 4. WLAN Resource Management

**4.1** The only design architecture permitted for GSFC WLANs is an infrastructure network that provides for an association between a specific access point and a connection to the wired LAN. *Ad hoc* networks are prohibited. The GSFC CIO's office may grant waivers in view of special circumstances on a case-by-case basis. A security assessment and impact report shall be prepared for each waiver granted. Following the format provided in [Appendix A](#) of this GPG, submit waiver requests to the Code 291 Customer Interface Team (CIT) where there is a Customer Service Manager (CSM) assigned for support of your organizational code. Your assigned CSM will then be responsible for processing the waiver request within Code 290 (waiver requests are acted on by the GSFC Code 290 CCB before presentation to the GSFC CIO), obtaining GSFC CIO approval, and for providing you with a signed memo conveying the results of the waiver request..

**4.2** GSFC WLANs and wireless access points shall utilize only GSFC Code 290 CCB approved equipment, configurations, and security controls. Users shall not install or use any WLANs or wireless access points without prior written approval by the GSFC Code 290 CCB. Paragraphs [8](#) and [9](#) of this GPG provide information on requesting GSFC Code 290 CCB approval.

**4.3** For GSFC guest-use of WLANs and wireless access points, all guest sessions through a wireless access point shall be logged, and limits shall be set for reachable destinations, the protocols to be used, the duration of access, and useable bandwidth. Waivers from the GSFC CIO's office are required for guest-use WLANs and wireless access points. Following the format provided in [Appendix B](#) of this GPG, submit guest use waiver requests to the Code 291 CIT where the CSM assigned to your Code will process it and provide you with written and signed results.

**4.4** All WLAN access points and wireless access points to wired LANs shall be physically secured such that only authorized personnel may gain physical access to wireless access devices. As a minimum, such access points and devices shall be protected by a locked door accessible by key or electronic device such as a keycard reader. Administrative logons shall be secured sufficiently to prevent unauthorized access to or tampering with the devices.

**4.5** The Radio Frequency transmission footprints of the WLAN access points shall be limited to the greatest extent possible to areas where authorized users are expected to reside.

**4.6** WLAN access points that have any connectivity to GSFC wired networks shall only be established on GSFC registered IP addresses.

**4.7** All WLAN access points and IP addresses shall be registered with the GSFC Code 290 CCB and comply with IP management requirements. The Enterprise IT Security Branch, Code 297, has the authority to deny and terminate access where non-compliant conditions are found.

**4.8** The GSFC Code 290 CCB is vested with the authority to set and adjust bandwidth limits for traffic between WLAN access points and wired networks.

**4.9** The C-ITSM is vested with the authority to disconnect or deny service to a mobile device in the event of an incident or a violation of acceptable use of wireless technology.

**4.10** Acting for the GSFC CIO, the GSFC Code 290 CCB will approve and document all network management protocols to be allowed for use on WLAN access points.

## **5. Spectrum Management**

To comply with federal laws, all non-licensed devices must be approved for legal conformance by the GSFC Frequency Manager (GSFC Code 450.0) before equipment is purchased. The GSFC Code 290 CCB shall verify its list of authorized wireless equipment with the GSFC Frequency Manager.

## **6. Monitoring**

**6.1** The GSFC CIO, through Code 297, shall establish procedures and schedules for the monitoring of GSFC WLAN access points on a regular basis for security, performance, traffic analysis, and vulnerabilities.

**6.2** Code 297 shall review authentication, authorization, and usage logs on a regular basis for unusual or suspicious activity.

**6.3** Any unusual wireless network event that may reflect unauthorized use of wireless network services shall immediately be reported by the WLAN System Administrator(s) to the C-ITSM for review and, if appropriate, investigation.

**6.4** Code 290 shall cause a full GSFC center-wide site survey to be performed on an annual basis to detect unauthorized WLANs and wireless access points. Spot checks shall be conducted on a quarterly basis.

## **7. Responsibilities**

**7.1** The GSFC CIO has overall responsibility to ensure that NASA GSFC data and systems are properly safeguarded from the inherent weaknesses of wireless data communication and is responsible for establishing policy and processes to ensure that

<b>DIRECTIVE NO.</b>	<u>GPG 2810.2</u>
<b>EFFECTIVE DATE:</b>	<u>July 9, 2004</u>
<b>EXPIRATION DATE:</b>	<u>July 9, 2009</u>

- a. Wireless network addresses are registered with Code 290;
- b. The GSFC Code 290 CCB maintains a list of approved wireless access point products;
- c. That GSFC is monitored for unauthorized access points;
- d. That GSFC personnel are advised of the risks associated with wireless data communication and are trained in the usage of appropriate safeguards and other related requirements and policies;
- e. That the C-ITSM has the authority to deny access and seize wireless equipment in violation of NASA and GSFC policies or where such equipment poses a risk to a GSFC wired network; and
- f. That waivers are documented with justification and include a security assessment and impact report.

**7.2** The C-ITSM shall develop, manage, and implement comprehensive processes and procedures for wireless security in accordance with NASA and GSFC policies and requirements; shall designate authorized personnel for the monitoring and reporting of wireless access usage; and shall provide necessary guidance and coordination with management in the enforcement of this policy.

**7.3** The GSFC Code 450 Center Frequency Manager is responsible for ensuring that GSFC's list of approved wireless equipment is in compliance with Federal requirements.

**7.4** Supervisors and managers are responsible for ensuring that wireless networks under their purview are in compliance with NASA and GSFC policies.

**7.5** Civil service and contractor employees are responsible for informing their guests and visitors of GSFC policies and procedures regarding wireless equipment.

**7.6** Individual civil service and contractor employees are responsible for becoming familiar with the provisions of this Goddard Procedures and Guidelines (GPG) and understanding the policies and procedural requirements pertaining to installation and use of wireless equipment on the GSFC campus and at GSFC managed facilities.

**7.7** Code 297 shall provide Initial Training to Directorate and Organizational Computer Security Officials (CSO). These CSOs, in turn, shall provide specific training to the personnel within their jurisdictions needing such training.

## **8. Requesting New Service**

**8.1** There is a GSFC initiative to procure and install a fully compliant wireless network infrastructure for the Goddard campus. The schedule for this initiative indicates that installation is to occur in phases, the plan, subject to funding, being to equip four or five buildings per year. Wireless services may be implemented by Code 290 in response to a customer request or by the customer itself. To request a new Code 290 or user implemented wireless service, the following steps need to be taken.

- a. Written Request. An organization, project, or function needing wireless access to its wired local area network submits a written request to the CIT of the NASA Communications Branch, GSFC/Code 291. That request will identify the customer by name, organization code, phone number, and email address. The request will include a statement wherein the customer agrees to fund, up front, the

implementation cost. The customer must then provide a detailed description of the wireless service being requested, including building and room numbers, and a brief operations concept in which are contained purpose, use, and intended users.

b. Solution. The written request will be assigned to a Code 291 CSM. The CSM works with the customer to ensure completeness of the requirement statement. The CSM then coordinates with the appropriate Network Engineer to develop a solution, prepare the documentation for GSFC Code 290 CCB approval, and provide a cost estimate for the implementation of that solution. After GSFC Code 290 CCB approval, a GSFC Code 290 CCB signed memo of CCB action is provided to the CSM for presentation, along with the cost estimate, to the customer for approval to proceed.

c. Funding. The customer, assuming acceptability of the proposed solution and the estimated cost for its implementation, is then asked to transfer funds in the amount indicated in the cost estimate to the Code 290 Resource Analyst. When the funds are received in good order, Code 291 will then proceed with its implementation.

d. Code 291 Implementation. When Code 291 is requested to do the implementation, it implements the solution proposed in its cost estimate and provides basic user training to the customer.

**8.2** User Implementation. For those situations where the customer will be implementing its own wireless solution, the customer is required to ensure that the implementation complies with the provisions of this GPG and with GSFC and NASA policies for wireless access to wired local area networks. To ensure the implementation is in compliance, the following steps shall be taken.

a. Written Request. The customer submits a written request to the CIT of the NASA Communications Branch, GSFC/Code 291, stating that it will procure and install the wireless access itself. The customer must submit a design and equipment list with its request to enable Code 291 to verify that the design and equipment are compliant with the GPG and NASA policies for wireless data access to local area networks. Additionally, the customer needs to provide a brief operations concept in which are contained purpose, use, and intended users. The customer shall not commence installation until after receipt of written approval from the GSFC Code 290 CCB.

b. Review and Approval. The CSM to whom the request is assigned sponsors its review by Code 291 engineering for design and by Code 297 for compliance with security policies and requirements. If the design and equipment list are determined to be compliant, then the CSM will prepare a written response to the customer in which are communicated the results of the review and authorization for the customer to proceed with procurement and installation. The response will also remind the customer of its continuing responsibility to maintain compliance with the provisions of this GPG and NASA wireless policies. If the design and/or the equipment are determined not to be in compliance with provisions of this GPG and NASA policies for wireless access, then Code 291 will advise the customer of the specific nature of the deficiencies, giving the customer an opportunity to make the necessary corrections. This may continue as an iterative process until such time as (1) the design and equipment list are approved or (2) a waiver has been granted for those non-conforming aspects of the design or equipment list. The customer shall not proceed with any aspects of the implementation until receipt of approval by the GSFC Code 290 CCB or of such waivers as may be necessary to allow implementation to proceed. The

results of the GSFC Code 290 CCB action will be conveyed in writing via a signed letter from the GSFC Code 290 CCB.

c. Implementation. Upon receipt of written GSFC Code 290 CCB approval or waivers, the customer may proceed with implementation. As-built drawings of the implementation shall be provided to Code 291 for audit and configuration management purposes. The customer's implementation becomes part of the installed base for which Code 290 is assigned management oversight responsibility.

**8.3** Assistance. If assistance in carrying out any of the requirements of paragraph 8 is required, contact the Code 291 Customer Interface Team (CIT) for support and guidance.

**8.4** WCNE. With the implementation of WCNE, much of this communication between customer and Code 290 is expected to be made possible via a dedicated Web site.

## **9. Requesting Approval of an Existing, User Installed Service**

**9.1** General Procedure. The Center recognizes that there are multiple *ad hoc* wireless systems installed and operating on-campus today. Such systems must be identified, and where not in compliance with NASA and GSFC policies and security requirements, actions taken to bring them into compliance or remove them from operation. Owners of pre-existing wireless networks and wireless access points to wired LANs shall notify Code 290 in writing of the existence of such networks and access points. Address each notification to GSFC/Code 291 Attention: Customer Interface Team. Each notification shall include a list of the installed equipment (make/model), protocols used, and a statement of what encryption is provided and whether it is turned on. Upon evaluation of the information contained in the notification and such other information as may be collected during the evaluation process, GSFC Code 290 CCB will respond in a formal letter advising the owner of the system's status and what additional actions, if any, are required and the time frame in which they must be completed for the system to continue operating.

**9.2** Certification. Owners of pre-existing wireless networks and wireless access points to wired data networks are required to audit their networks and certify to the extent of compliance with this GPG and NASA policies governing wireless data transmission. More specifically, each area of questionable or actual non-compliance shall be identified and accompanied by a corrective action statement or plan.

**DIRECTIVE NO.** GPG 2810.2  
**EFFECTIVE DATE:** July 9, 2004  
**EXPIRATION DATE:** July 9, 2009

## Appendix A. Waiver Request for GSFC WLAN

### A. Organization Requesting Waiver

Name: \_\_\_\_\_

Org Code: \_\_\_\_\_ Building: \_\_\_\_\_ Room: \_\_\_\_\_

Time Period of Waiver \_\_\_\_\_

### B. Justification for waiver (may attach a separate sheet)

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

### C. Impact of not granting the waiver (May attach a separate sheet)

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

### D. Security Assessment (May attach a separate sheet)

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

### E. Approvals

Organization Approval (Branch Chief or higher)

\_\_\_\_\_  
Name Signature Date

Chief Information Officer's Approval

\_\_\_\_\_  
Name Signature Date

**DIRECTIVE NO.** GPG 2810.2  
**EFFECTIVE DATE:** July 9, 2004  
**EXPIRATION DATE:** July 9, 2009

## Appendix B. Waiver Request for Guest Use of GSFC WLAN/Wireless Access Points

### A. Organization Requesting Waiver

Name: \_\_\_\_\_ Org Code: \_\_\_\_\_

Location of WLAN Building: \_\_\_\_\_ Room: \_\_\_\_\_

### B. Personal Information

Name of Guest \_\_\_\_\_ Citizenship \_\_\_\_\_

### C. Purpose of Visit

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Date (s) of Visit \_\_\_\_\_

Time Period of Waiver \_\_\_\_\_

### D. System Information

Request waiver for wireless access to the following System(s)

Name	Org Code	Location
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

### E. Approvals

Organization Approval (Branch Chief or higher)

\_\_\_\_\_  
Name Signature Date

Chief Information Officer's Approval

\_\_\_\_\_  
Name Signature Date

