



Nett Warrior



Security Classification Guide




November 29, 2011

DISTRIBUTION C: Distribution authorized to U.S. Government Agencies and their contractors only, for protection of technical and operational information, effective the approval date of this document. Other requests for this document shall be referred to Project Manager Soldier Warrior, ATTN: SFAE-SDR-SWAR, Fort Belvoir, VA 22060

This document contains information EXEMPT FROM MANDATORY DISCLOSURE under the Freedom of Information Act (FOIA). Exemption 2 applies.


FOR OFFICIAL USE ONLY

Nett Warrior Security Classification Guide

Submitted by: 

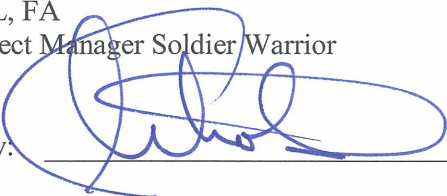
Date 9 Dec 2011

ROLAND M. GADDY, JR.
LTC, IN
Product Manager Ground Soldier

Concurred by: 

Date 12 Dec 2011

DAVID W. RIGGINS
COL, FA
Project Manager Soldier Warrior

Approved by: 

Date 27 Dec 11

CAMILLE M. NICHOLS
Brigadier General, USA
Program Executive Officer Soldier

Revision: This Security Classification Guide (SCG) is a revision to the Ground Soldier System SCG, approved 17 Aug 07.

Action Officer: Mr Jeff Witherel
Project Manager Soldier Warrior
SFAE-SDR-SWAR
10125 Kingman Road, Bldg 317
Fort Belvoir, VA 22060-5820
(703) 704-3860
DSN: 654-3860

SUMMARY of CHANGE

This revision:

- Updates information on the Office of Primary Responsibility (OPR).
- Replaces the term Government Furnished Property (GFP) vice Government Furnished Equipment (GFE) for accuracy.
- Corrects the program description to reflect Nett Warrior (NW) vice Ground Soldier System (GSS).
- Changes the Classification Matrices as follows:
 - Section III, Performance and Capabilities
 - Changes Operational Range of Radios to Operational Range of Transport System and appropriate Remarks.
 - Changes Radio Frequencies to Radio Spectrum and appropriate Remarks.
 - Section V, Hardware/Software
 - Changes Ground Soldier System Specific Hardware to Nett Warrior Specific Hardware. Lists NW hardware with appropriate Remarks.
 - Under Software section, changes GSS software compiled code to NW system software source code and corresponding Remarks; and provides handling instructions in Remarks for Encryption Keys.
- Updates Section X, References

SECTION I – GENERAL INFORMATION

1. Purpose.

To provide instructions and guidance on the security classification of information and materiel pertaining to the Nett Warrior (NW) program. It is a revision to the Ground Soldier System Security Classification Guide (SCG), approved 17 Aug 07.

2. Authority.

This guide is issued under the authority of AR 380-5, Department of the Army Information Security Program; DoD 5200.1R, Information Security Program; and Executive Order (EO) 13526, Classified National Security Information. This guide constitutes original determination by authority of the Program Executive Officer Soldier (PEO SDR), and may be cited as the basis for classification, re-grading, or declassification of information for the NW program. Changes are effective immediately.

3. Office of Primary Responsibility (OPR).

This guide is issued by, and all inquiries concerning content and interpretation, as well as any recommendations for changes, should be addressed to:

**Project Manager Soldier Warrior
SFAE-SDR-SWAR
Fort Belvoir, VA 22060**

**Action Officer:
Mr. Jeff Witherel
10125 Kingman Road, Bldg 317
Fort Belvoir, VA 22060-5820
(703) 704-3860
DSN: 654-3860**

4. Classification Challenges.

Questions concerning the content and interpretation of this guide should be directed to the issuing activity. If the security classification imposed by this guide is considered impractical, documented and justified recommendations should be made through appropriate channels to the issuing activity. If current conditions, progress made in this effort, scientific or technological developments, advances in the state-of-the-art, or other factors indicate a need for changes, similar recommendations should be made. Pending a final decision, the information involved will be protected at either the currently specified level or the recommended level, whichever is higher. All users of this guide are encouraged to assist in improving its currency and adequacy. Any classification challenges should be brought to the attention of the OPR.

5. Reproduction, Extraction, and Dissemination.

Copies of this guide and all extracts thereof will be made, stored, and transmitted IAW authorized procedures corresponding to the classification of the information involved. Authorized recipients of this guide may reproduce, extract, and disseminate the contents of this guide, as necessary, for use by specified groups, including industrial activities that are involved in Nett Warrior system development, test, or operation. Requests for copies of separate guides issued to operating activities in application of this guide shall be sent to the OPR.

6. Public Release.

The fact that certain details of information are shown to be unclassified does not authorize automatic public release. Proposed public releases of unclassified information related to the NW program must be processed through appropriate channels for approval for publication. Within the Department of the Army, the procedures specified in AR 360-1, The Army Public Affairs Program, will be followed. Defense contractors will comply with DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), and other contractual requirements. All information concerning the NW will be forwarded for public clearance to the PEO Soldier Operations and Communications Directorate, in accordance with AR 360-1, Chapter 5 and Appendix D.

7. Foreign Disclosure.

Any disclosure to foreign officials of information classified by this guide shall be in accordance with the procedures set forth in AR 380-10, Foreign Disclosure and Contacts with Foreign Representatives, and National Disclosure Policy, NDP-1. If a country with which the Department of Defense has entered into a reciprocal procurement memorandum of understanding or offset arrangement expresses an interest in a solicitation that will eventually involve the disclosure of US classified military information, a foreign disclosure review and adjudication should be conducted prior to issuance of a solicitation. If it is known that foreign participation cannot be permitted because of the sensitivity of the effort, this fact should be stated.

8. Foreign Government Information and Foreign Military Sales.

The safeguarding of Foreign Government Information (FGI) will be in accordance with DoD 5220.22M, AR 380-5 and the provisions of DoD 5105.38-M, Security Assistance Management Manual (SAMM), apply. The provisions of AR 380-5 apply to the proper security classification marking and protection of any foreign government information. Specific international agreements on security of military information may also apply.

Highest security classification of information that will be necessary to be disclosed in support of the end item sale of the NW is SECRET.

If a foreign country expresses an interest to enter into a reciprocal procurement or other offset arrangement for this project with the or a defense contractor, whether Foreign Military Sales (FMS) or a commercial program, the OPR shall be notified without delay.

9. Derivative Security Classification and Handling Instructions.

Project Manager (PM) Soldier Warrior will comply with the security classification markings and handling instructions of information incorporated into the program from external sources, e.g., Government Furnished Property (GFP). Specifically, the PM will classify all information from external sources according to the appropriate security classification guidance. These provisions will apply particularly to communications security information, which will be classified according to National Security Agency security classification guidance. Note that the applicable PM must be contacted on questions pertaining to any GFP items that do not have a security classification guide.

10. For Official Use Only (FOUO) Caveat.

For Official Use Only is not a security classification. Information that has not been given a security classification pursuant to the criteria in this guide, but which may be withheld from the public for one or more of the reasons cited in the Freedom of Information Act (FOIA) exemptions in AR 25-55, Army Freedom of Information Act Program, shall be designated FOUO. Information so designated in this guide that warrants FOUO markings will be handled and protected in accordance with the above-cited regulation. Documents will be marked “FOR OFFICIAL USE ONLY” in letters larger than the rest of the text, where practical, at the bottom of the front cover, the title page, or the first page, and the outside of the back cover. Pages within the document which contain FOUO information will be marked “FOR OFFICIAL USE ONLY” at the bottom. The following statement will be applied to the front cover or title page of the document with the appropriate exemption(s) identified:

“This document contains information EXEMPT FROM MANDATORY DISCLOSURE under the Freedom of Information Act (FOIA). Exemption(s) . . . applies/apply.”

FOIA exemptions identified in this guide are as follows:

- Number 2 Related solely to the internal personnel rules and practices of DoD and its Components. Records containing or constituting statutes, rules, regulations, orders, manuals, directives, instructions, and security classification guides.
- Number 3 Records protected by another law that specifically exempts the information from public release. Applicable to technical Controlled Unclassified Information.
- Number 4 Information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis that, if released, would result in competitive harm to the company, impair the Government’s ability to obtain like information in the future, or protect the Government’s interest in compliance with program effectiveness.
- Number 5 Inter-Agency memoranda that are deliberative in nature; this exemption is appropriate for internal documents that are part of the decision making process and contain subjective evaluations, opinions, and recommendations.

Note that the listed exemptions are examples and not all inclusive. The user should review AR 25-55 for all exemption guidance.

11. Reasons for Classifying.

The reasons for classifying information in this guide are in accordance with Part I, Section 1.4, Executive Order 13526. They are:

- 1.4a - Military plans, weapons systems, or operations.
- 1.4e - Scientific, technological, or economic matters related to the National Security, which includes defense against transnational terrorism.
- 1.4g - Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the National Security, which includes defense against transnational terrorism.

12. Program Description.

NW is managed and developed by Product Manager Ground Soldier (PdM GS) under Project Manager Soldier Warrior (PM SWAR) and PEO Soldier (PEO SDR) at Ft Belvoir, VA. The program is currently in the Technology Development (TD) Phase. At the conclusion of the TD Phase, it will transition to Low Rate Initial Production (LRIP).

NW is a Soldier-worn dismounted mission command system that supports the mission of the dismounted combat leader. The NW capabilities are informed by various Army demonstration, test and evaluation events, including Network Integration Evaluation (NIE), Army Expeditionary Warfighter Experiment (AEWE) activities and combat experiences from the preceding Soldier system called the Land Warrior (LW) system.

The NW is intended to address operational requirements to provide the dismounted Leader with improved situational awareness, command and control capabilities. It links the dismounted leader via voice and data communications to Soldiers at the Tactical Edge and to headquarters at platoon and company levels. The NW requirements translate into the user being at the right place, at the right time, with the right equipment, using near real-time information to be more effective and more lethal executing their combat missions. NW will provide this capability with an affordable, tailored system approach that provides required operational capabilities by position within the echelon.

13. Classification Matrices.

The following Sections II through IX matrices provide the classification of each item or element of the program. Classification level and /or handling instructions (in the Remarks column) are provided as well as the duration of the classification and downgrading instructions.

SECTION II – OVERALL EFFORT

Element	Level	Duration	Remarks
Program name	U		
Program description	U		
Component or subcomponent nomenclature	U		
Program goals, mission, and purpose	U		
Operational requirements to include key performance parameter(s)	U		

SECTION III - PERFORMANCE AND CAPABILITIES

Element	Level	Duration	Remarks
<p>General information regarding the capabilities of the NW system</p> <p>Note: This section includes components that are Government Furnished Property (GFP) and Commercial Off The Shelf (COTS)</p>	<p align="center">U</p>		<p>General Information refers to information that has been approved for public release by PEO Soldier Operations and Communications Directorate.</p>
<p>Specific details regarding the capabilities of the NW system, subsystems, and components</p> <p>Note: This section includes NW components that are GFP and COTS</p>	<p align="center">See Remarks</p>	<p align="center">Declassify 10 years from date of system fielding</p>	<p>If component specific classification guide exists, then classify in accordance with that guidance</p> <p>Specific information not covered in a component classification guide is treated as:</p> <p>CONFIDENTIAL if loss of information would reveal or compromise a future capability, or if a new application of existing technology is revealed which would compromise an enhanced system capability</p> <p>SECRET if loss of information would allow an adversary to deny, degrade, deceive, disrupt, or destroy the NW system or subsystems, or if</p>

			<p>details would lead to loss of research, development, and engineering; scientific; or technical information that would lead to a tactical disadvantage</p> <p>UNCLASSIFIED if the above thresholds are not met. Mark and handle as FOUO, FOIA exemptions 4 and/or 5 apply</p>
Operational range of transport system	See Remarks		Classify in accordance with the applicable system classification guide
Radio spectrum	See Remarks		Classify in accordance with the applicable system classification guide
Specific COTS/GFP component performance	See Remarks		Classify in accordance with the applicable system classification guide

SECTION IV – SPECIFICATIONS

Element	Level	Duration	Remarks
<p>System Performance Specifications and Subsystem Product Specifications</p> <p>Note: This section includes NW system components that are GFP and COTS</p>	See Remarks	Declassify 10 years from date of system fielding	<p>If component specific classification guide exists, then classify in accordance with that guidance</p> <p>Specific information not covered in a component classification guide is treated as:</p> <p>Test data and operational test data are classified SECRET if countermeasures, counter</p>

			<p>countermeasures, vulnerabilities, and/or weaknesses are revealed that could reduce the operational effectiveness of the NW system</p> <p>Interface control documents are UNCLASSIFIED except for specific cryptographic devices that are SECRET//NOFORN. The COMSEC portions only are NOFORN.</p> <p>UNCLASSIFIED if the above thresholds are not met. Mark and handle as FOUO, FOIA exemptions 4 and/or 5 apply</p>
Power Requirements	U		
Physical Characteristics (size, weight, shape)	U		

<p>Quality Assurance</p>	<p>See Remarks</p>	<p>Declassify 10 years from date of system fielding</p>	<p>If component specific classification guide exists, then classify in accordance with that guidance</p> <p>Specific information not covered in a component classification guide is treated as:</p> <p>Test data and operational test data are classified SECRET if countermeasures, counter countermeasures, vulnerabilities, and/or weaknesses are revealed that could reduce the operational effectiveness of the NW system</p> <p>UNCLASSIFIED if the above thresholds are not met. Mark and handle as FOUO, FOIA exemptions 4 and/or 5 apply.</p>
<p>Technical Drawings</p> <p>Note: This section includes NW system components that are GFP and COTS</p>	<p>See Remarks</p>	<p>Declassify 10 years from date of system fielding</p>	<p>If component specific classification guide exists, then classify in accordance with that guidance</p> <p>Specific information not covered in a component classification guide is treated as:</p> <p>CONFIDENTIAL if loss of information would reveal or compromise a future capability, or if a new application of existing technology is revealed which would compromise an enhanced system capability</p> <p>SECRET if countermeasures, counter countermeasures, vulnerabilities, and/or weaknesses are revealed that could reduce the operational effectiveness of the NW system, or if details would lead to loss of research,</p>

			development, and engineering; scientific; or technical information that would lead to a tactical disadvantage UNCLASSIFIED if the above thresholds are not met. Mark and handle as FOUO, FOIA exemptions 3, 4 and/or 5 apply.
Interface Control Documents	See Remarks		Interface control documents are UNCLASSIFIED except for specific cryptographic devices that shall be handled, marked and safeguarded in accordance with policies and procedures of the National Security Agency

SECTION V - HARDWARE / SOFTWARE

Element	Level	Duration	Remarks
General description of technologies used in the NW system Note: This section includes NW system components that are GFP and COTS	U		General information refers to information that has been approved for public release by PEO Soldier Strategic Communications Office.
Specific technical details of technologies being used in the NW system Note: This section includes NW system components that are GFP and COTS	See Remarks	Declassify 10 years from date of system fielding	If component specific classification guide exists, then classify in accordance with that guidance Specific information not covered in a component classification guide is treated as: CONFIDENTIAL if loss of information would reveal or compromise a future capability, or if a

			<p>new application of existing technology is revealed which would compromise an enhanced system capability</p> <p>SECRET if loss of information would allow an adversary to deny, degrade, deceive, disrupt, or destroy the NW system or subsystems, or if details would lead to loss of research, development, and engineering; scientific; or technical information that would lead to a tactical disadvantage</p> <p>UNCLASSIFIED if the above thresholds are not met. Mark and handle as FOUO, FOIA exemptions 4 and/or 5 apply.</p>
External / Internal Views			
<p>Images, drawings, and schematics of the external view of the NW system, subsystems, or components</p> <p>Note: This section includes NW system components that are GFP and COTS</p>	U		<p>If component specific classification guide exists, then classify in accordance with that guidance</p>
<p>Images, drawings, and schematics of the internal view of the NW system, subsystems, or components</p> <p>For technical drawings refer to Section IV - Specifications</p> <p>Note: This section includes NW</p>	See Remarks		<p>If component specific classification guide exists, then classify in accordance with that guidance</p> <p>Specific information not covered in a component classification guide: Mark and handle as FOUO, FOIA exemptions 4 and/or 5 apply.</p>

system components that are GFP and COTS			
Nett Warrior Specific Hardware			
End User Device	See Remarks		Hardware is unclassified.
Interconnect Cable	U		
Other Ancillary Equipment	U		
Vehicle integration kit	U		
Commercial Off the Shelf (COTS) / Government Furnished Property (GFP)			
Fact that the NW system uses COTS/GFP systems	U		
Association of COTS/GFP with a specific NW system subsystem or component	U		Association of a specific radio/wave form/digital network with the NW system is marked and handled as FOUO
Modification of COTS/GFP	See Remarks	Declassify 10 years from date of system fielding	Classify in accordance with the applicable system classification guide Specific information not covered in a component classification guide: CONFIDENTIAL if new application of existing technology is revealed which would compromise an enhanced system capability, or if a new application of existing technology is revealed which would compromise an enhanced system capability SECRET if details would lead to loss of research,

			<p>development, and engineering; scientific, or technical information that would lead to a tactical disadvantage</p> <p>UNCLASSIFIED if the above threshold is not met. Mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.</p>
Radio	See Remarks		Classify in accordance with the applicable system classification guide
Software			
<p>NW system software source code</p> <p>Developmental Items (Ex: interface software, Map interface, comms suite, security software, etc.)</p> <p>Non-Developmental Items (Ex: map engines, database engine, operating systems, parser, security software, etc.)</p>	See Remarks	<p>Declassify 10 years from date of system fielding</p>	<p>The NW system source code is UNCLASSIFIED; however, a detected vulnerability in the source code is treated as SECRET.</p> <p>UNCLASSIFIED if the above threshold is not met. Mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.</p>
<p>Information Assurance technical details</p> <p>(To include network intrusion detection system, key fill bus, firewall, and switches)</p>	See Remarks	<p>Declassify 10 years from date of system fielding</p>	<p>If component specific classification guide exists, then classify in accordance with that guidance</p> <p>Specific information not covered in a component classification guide is treated as:</p> <p>CONFIDENTIAL if loss of information would reveal or compromise a future capability, or if a new application of existing technology is revealed which would compromise an enhanced system capability</p>

			<p>SECRET if details would lead to loss of research, development, and engineering; scientific, or technical information that would lead to a tactical disadvantage</p> <p>UNCLASSIFIED if the above thresholds are not met. Mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.</p>
Cryptographic capabilities and equipment associated with NW system communication and networking components	See Remarks		<p>Encryption Keys are handled as SECRET when readable as plain text.</p> <p>COMSEC material and Controlled Cryptographic Items shall be handled, marked, and safeguarded in accordance with policies and procedures of the National Security Agency.</p> <p>Contact OPR, i.e., National Security Agency</p>

SECTION VI – ADMINISTRATIVE

Element	Level	Duration	Remarks
Funding requirements	U		Mark and handle as FOUO, FOIA exemption 2 applies
Budget data	U		Information released yearly by the President's Budget Submit and associated forms is public information and is UNCLASSIFIED, distribution statement A – public release

			For all other budget data, mark and handle as FOUO, FOIA exemption 2 applies
Quantities	U		Information released yearly by the President's Budget Submit and associated forms is public information and is UNCLASSIFIED, distribution statement A – public release For all other quantities, mark and handle as FOUO, FOIA exemption 2 applies
Unit cost	U		Information released yearly by the President's Budget Submit and associated forms is public information and is UNCLASSIFIED, distribution statement A – public release For all other cost data, mark and handle as FOUO, FOIA exemption 2 applies
Program and production schedule	U		Mark and handle as FOUO, FOIA exemption 2 applies
First Unit Equipped (FUE) date	U		FUE date by itself is unclassified. FUE date associated with a specific unit, at a minimum, mark and handle as FOUO, FOIA exemption 2 applies, and may require a higher classification level based upon unit requirements.
Initial Operational Capability (IOC) date	U		IOC date by itself is unclassified. IOC date associated with a specific unit, at a minimum, mark and handle as FOUO, FOIA exemption 2 applies, and may require a higher classification level based upon unit requirements.

Identification of NW system units	U		Mark and handle as FOUO, FOIA exemption 2 applies
Basis of issue	U		
Acquisition strategy/acquisition plan	U		Mark and handle as FOUO, FOIA exemption 2 applies
Contract performance requirements	U		Mark and handle as FOUO, FOIA exemption 2 applies

SECTION VII - VULNERABILITIES AND WEAKNESSES

Element	Level	Duration	Remarks
Details of specific operational limitations of the NW system or subsystems	See Remarks	Declassify 10 years from date of system fielding	Classify in accordance with the applicable system classification guide Specific information not covered in a component classification guide that could allow an adversary to deny, degrade, deceive, disrupt, or destroy the NW system or subsystems is SECRET
Vulnerability to Electronic Countermeasures (ECM)/Electronic Support Measures (ESM)	S	Declassify 10 years from date of system fielding	
Countermeasure methods of degrading operational effectiveness of system	S	Declassify 10 years from date of system fielding	
Counter countermeasures	S	Declassify 10	

		years from date of system fielding	
Vulnerability and susceptibility to physical attack including Directed Energy Warfare (DEW) and Nuclear, Biological, and Chemical (NBC) attack	S	Declassify 10 years from date of system fielding	
TEMPEST	See Remarks		Information concerning cryptographic TEMPEST vulnerabilities must be classified SECRET.

SECTION VIII - TEST AND EVALUATION

Element	Level	Duration	Remarks
Details of the NW system or subsystem test plan	U		Mark and handle as FOUO, FOIA exemption 2,4 or 5 applies
Identification of specific test locations associated with the NW system or subsystems	U		Mark and handle as FOUO, FOIA exemption 2,4 or 5 applies Information is UNCLASSIFIED upon completion of test
Test data	See Remarks	Declassify 10 years from date of system	Test data is to be classified in accordance with the information revealed. Test data that indicates/reveals vulnerabilities/susceptibilities are

		fielding	classified in accordance with other sections of this classification guide (Sections V/VII). Information that is UNCLASSIFIED will be marked and handled as FOUO, FOIA exemption 4 and/or 5 applies
--	--	----------	---

SECTION IX – MAINTENANCE

Element	Level	Duration	Remarks
Identification and/or location of specialized maintenance organizations associated with the NW system	See Remarks		Classify in accordance with the applicable system classification guide Specific information not covered in a component classification guide: Mark and handle as FOUO if FOIA exemption 4 and/or 5 applies
Maintenance that reveals specific system information (e.g. design, development, capabilities, vulnerabilities, etc.)	See Remarks		Classify in accordance with the applicable system classification guide Specific information not covered in a component classification guide: Mark and handle as FOUO if FOIA exemption 4 and/or 5 applies
Reliability, Availability, Maintainability (RAM)	U		Mark and handle as FOUO if FOIA exemption 4 and/or 5 applies
Integrated Logistics Support	U		Mark and handle as FOUO if FOIA exemption 4 and/or 5 applies

SECTION X - REFERENCES

1. Executive Order 13526, Classified National Security Information, 29 December 2009
2. AR 25-55, Department of the Army Freedom of Information Act Program, 1 November 1997
3. AR 360-1, The Army Public Affairs Program, 25 May 2011
4. AR 380-5, Department of the Army Information Security Program, 29 September 2000
5. National Disclosure Policy (NDP-1), 1 October 1988.
6. AR 380-10, Foreign Disclosure and Contacts with Foreign Representatives, 22 June 2005.
7. DoD 5105.38-M, Security Assistance Management Manual, 3 October 2003
8. DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), 6 February 2006
9. DoDD 5230.25, Withholding of Unclassified Technical Data from Public Disclosure, 16 November 1984; Change 1, 18 August 1995
10. DoDD 5230.24, Distribution Statements on Technical Documents, 18 March 1987
11. DoD Pamphlet 5230.25-PH, Control of Unclassified Technical Data with Military or Space Application, May 1985
12. DoD 5200.1-R, Information Security Program, 14 January 1997
13. National Telecommunications and Information Systems (NTISSI) 4002, Classification Guide for COMSEC Information, 5 June 1986.
14. Security Classification Guide Joint Tactical Radio System Cluster 5, 2 August 2004
15. Security Classification Guide for Force XXI Battle Command Brigade and Below (FBCB2)/Joint Battle Command-Platform (JBC-P), 31 March 2010.