SANDIA REPORT
SAND2012-0110
Unlimited Release
Printed January 2012

An Analysis of Department of Defense Instruction 8500.2 'Information Assurance (IA) Implementation'

Philip L. Campbell

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Approved for public release; further dissemination unlimited

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from

U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from

U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2012-0110
Unlimited Release
Printed January 2012

An Analysis of Department of Defense Instruction 8500.2 'Information Assurance (IA) Implementation'

Philip L. Campbell
Network Systems Survivability and Assurance
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-0672

Abstract

The Department of Defense (DoD) provides its standard for information assurance in its Instruction 8500.2, dated February 6, 2003. This Instruction lists 157 "IA Controls" for nine "baseline IA levels." Aside from distinguishing IA Controls that call for elevated levels of "robustness" and grouping the IA Controls into eight "subject areas" 8500.2 does not examine the nature of this set of controls, determining, for example, which controls do not vary in robustness, how this set of controls compares with other such sets, or even which controls are required for all nine baseline IA levels. This report analyzes (1) the IA Controls, (2) the subject areas, and (3) the Baseline IA levels. For example, this report notes that there are only 109 core IA Controls (which this report refers to as "ICGs"), that 43 of these core IA Controls apply without variation to all nine baseline IA levels and that an additional 31 apply with variations. This report maps the IA Controls of 8500.2 to the controls in NIST 800-53 and ITGI's COBIT. The result of this analysis and mapping, as shown in this report, serves as a companion to 8500.2. (An electronic spreadsheet accompanies this report.)

ACKNOWLEDGMENTS

Thank you to Edward L. Witzke, Mayuri Shakamuri, and Robert K. Zaring, all of Sandia National Laboratories, for their review.

CONTENTS

Acknowledgments 4

Contents 5

Figures 7

Tables 8

Acronyms 12

1 Introduction 13

2 Foundation 15

3 Analysis of IA Controls 29

3.1 Type 32

3.1.1 Signatures 32

3.1.2 Signature Patterns 37

3.1.3 Allowable Signatures 42

3.1.4 Partition Table 46

3.2 CIA 49

3.3 Span 53

3.4 Impact 57

3.5 Family 63

3.6 Class 74

3.7 Coverage 78

4 Analysis of subject areas 89

4.1 First Step: Subject Area Correspondence 90

4.1.1 Type 90

4.1.2 CIA 90

4.1.3 Span 91

4.1.4 Impact 91

4.1.5 Family 92

4.1.6 Class 94

4.1.7 Coverage 95

4.2 Second Step: Subject Area Correspondence 97

5 Analysis of Baseline IA Levels 100

5.1 First Step: Identify ICG and Robustness Communities 100

5.2 Second Step: Combine ICG and Robustness Communities 106

6 Summary 109

References 111

7 Appendix A: Gallery of Unusual ELements 113

8 Appendix B: IACs 114

9 Distribution 136

FIGURES

Figure 1 Impact Poset 58

Figure 2 Coverage Correspondence Sets 96

Figure 3 ICGs Category Differentials 104

Figure 4 Robustness Category Differentials 105

Figure 5 Combined Category Differentials 107

TABLES

Table 1 Example of an IA Control 15

Table 2 Subject Areas 16

Table 3 Assigned IA Controls by Mission Assurance Category and Confidentiality Level 18

Table 4 Attachments and IACs 19

Table 5 IACs in Each Baseline IA level 19

Table 6 IA Control Sets 22

Table 7 ICGs, Sorted on ICG Index 23

Table 8 ICGs, Sorted Alphabetically on ICG 26

Table 9 Candidate Partitions in 8500.2 31

Table 10 Partition Table, Sorted on Type (Fragment) 31

Table 11 ICG Types 33

Table 12 IAC-Unique Appearances and ICG Signatures & Types 34

Table 13 Non-Conforming ICGs 38

Table 14 Robustness Levels for Signature 11-1-- 40

Table 15 Robustness Levels for Equivalent Signatures 221211 and 2212-- 40

Table 16 Robustness Levels for Signature 2213-- 41

Table 17 Non-Conforming ICGs (Summary) 42

Table 18 Allowable Half Signatures 44

Table 19 Half Signatures (and Types) 45

Table 20 Coverage of Allowable Signatures 45

Table 21 Partition Table, Sorted on Type 46

Table 22 CIA Breakdown 49

Table 23 CIA Non-Conforming ICGs 49

Table 24 Partition Table, Sorted on CIA 50

Table 25 Span Breakdown 53

Table 26 Span 3 ICGs 53

Table 27 Span & Type 54

Table 28 Partition Table, Sorted on Span 54

Table 29 Impact Priorities Breakdown 58

Table 30 Impact Priority E ICGs 59

Table 31 Impact Priority Z ICGs 59

Table 32 Partition Table, Sorted on Impact 59

Table 33 NIST 800-53 Structure 64

Table 34 Mapping ICGs to NIST 800-53 Families 65

Table 35 ICG-to-NIST Mapping 66

Table 36 Partition Table, Sorted on Family 70

Table 37 Class Breakdown 75

Table 38 Partition Table, Sorted on Class 75

Table 39 CoBIT Structure 78

Table 40 Mapping ICGs to the CoBIT Domains 79

Table 41 Mapping ICGs to CoBIT Domains and Processes 79

Table 42 Mapping ICGs to CoBIT Process DS5 81

Table 43 ICG-to-CoBIT Mapping 81

Table 44 Partition Table, Sorted on Coverage 85

Table 45 Correspondence Grade Ranges 89

Table 46 Illustration: Correspondence with Partition X 90

Table 47 Correspondence with Type 90

Table 48 Correspondence with CIA 91

Table 49 Correspondence with Span 91

Table 50 Correspondence with Impact 91

Table 51 Correspondence with Family 92

Table 52 Combined Families 92

Table 53 Correspondence with Family (Combined) 93

Table 54 Correspondence with Class 95

Table 55 Correspondence with Coverage 96

Table 56 Correspondence Summary 97

Table 57 Robustness Levels for ICG ECTB (Signature 11-1--) 101

Table 58 Robustness Levels for ICG DCSS (Signature 2212--) 101

Table 59 ICG and Robustness Additions 102

Table 60 Basic Differentials 103

Table 61 ICG Category Differentials 104

Table 62 ICG Communities 105

Table 63 Robustness Category Differentials 105

Table 64 Robustness Communities 106

Table 65 Base Differentials (Combined) 106

Table 66 Category Differentials (Combined) 107

Table 67 Combined Communities 107

Table 68 IACs, Sorted on Appearance Index 114

Table 69 IACs, Sorted on Attachment within IA Control Number (IACN) 124

ACRONYMS

800-53	NIST 800-53 [10] (shorthand used in this report)
8500.2	DoDI 8500.2 [3] (shorthand used in this report)
CIA	Confidentiality, Integrity, Availability
CoBIT	Control Objectives for IT and Related Technology [1]
DoD	Department of Defense
FIPS	Federal Information Processing Standards ([6], [7])
IA	Information Assurance
IAC	IA Control
IACN	IA Control Number, e.g., ECCT-1
ICG	IA Control Group. For example, CODB-1, CODB-2, and CODB-3 are all in the CODB ICG
ISACA	(formerly) Information Systems Audit and Control Association [8]
IT	Information technology
ITGI	IT Governance Institute (www.itgi.org) [9]
MAC	Mission Assurance Category
NIST	National Institute of Standards and Technology
SAMI	Sources And Methods Intelligence

1 INTRODUCTION

From the time of its publication on February 6, 2003, the Department of Defense (hereafter DoD) Instruction 8500.2 "Information Assurance (IA) Implementation" [3] (hereafter 8500.2) has provided the definitions and controls that form the basis for IA across the DoD.

There are three interesting aspects of 8500.2 that bear analysis:

1. the IA Controls (IACs),
    - for example,
        i. COBR-1
        ii. ECCT-1
2. the IA Control "subject areas"
    - for example
        i. Enclave and Computing Environment (EC)
        ii. Security Design & Configuration (DC)
3. the baseline IA levels
    - for example
        i. MAC I Classified
        ii. MAC II Sensitive.

This report provides analysis of all three aspects.

8500.2 lists

- 157 IA Controls[1]
- in eight IA Control subject areas
- for nine baseline IA levels.

Aside from distinguishing IACs that call for elevated levels of "robustness" and noting whether a given IAC applies toward confidentiality, integrity, or availability, 8500.2 does not otherwise examine the nature of this set of controls or the subject areas or the baseline IA levels or the relationships between them. Concerning the IACs, 8500.2 does not determine, for example,

- how many IACs are the same across all nine baseline IA levels,
- how many IACs have the highest robustness level,
- how the set of IACs in 8500.2 compares with other sets, such as NIST's 800-53 [10].

The analysis provided in this report notes, for example, that

- 43 IACs are the same across all nine baseline IA levels,
- 7 IACs have the highest robustness level, and
- almost half of the IACs fit within one of the 210 control objectives of CobiT® [1].[2]

[1] As we will see in the subsequent section, this is the set "IAC-Unique."

The significance of these items will become apparent as the reader proceeds through the report.

The next section provides foundation material about 8500.2. The subsequent three sections present analysis of the IACs, the subject areas, and the baseline IA levels, respectively. A summary follows those sections. Finally, Appendix A presents a gallery of "unusual" elements of 8500.2, where "unusual" means that these elements have some characteristics shared by only a few other elements, and Appendix B lists the IACs.

---

[2] That one control objective is DS5 "Ensure systems security."

2 FOUNDATION

This section provides foundation material upon which the subsequent sections build.

8500.2 defines an IAC as follows:

> E2.1.26. IA Control. An objective IA condition of integrity, availability, or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities that is expressed in a specified format (i.e., a control number, a control name, control text, and a control class). Specific management, personnel, operational, and technical controls are applied to each DoD information system to achieve an appropriate level of integrity, availability, and confidentiality in accordance with OMB Circular A-130 (reference (v)). (8500.2, page 20)

An example of the parts of an IAC is shown in the following table, reproduced from 8500.2.[3]

Table 1 Example of an IA Control

IA Control Part	Example
IA Control Subject Area	Enclave and Computing Environment
IA Control Number	ECCT-1
IA Control Name	Encryption for Confidentiality (Data in Transit)
IA Control Text	Unclassified, sensitive data transmitted through a commercial or wireless network are encrypted using NIST-certified cryptography.

There is a discrepancy between the definition and the example, both shown above: the definition does not mention "subject area" and the example does not mention "control class." This report resolves this discrepancy by assuming that "subject area" is the fourth part of the IAC "format" and that "control class" refers to the unnamed set {management, personnel, operational, technical} shown in the definition, as though the definition were edited as follows, where the italicized text replaces the strikethrough text

> E2.1.26. IA Control. An objective IA condition of integrity, availability, or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities that is expressed in a specified format (i.e., a control number, a control name, control text, and a ~~control class). Specific management, personnel, operational, and technical controls~~ *subject area). There are four classes of IA Controls, namely management, personnel, operational, and technical. IA Controls* are applied to each DoD information system to achieve an appropriate level of integrity, availability,

[3] This table is the substance of Figure E4.F1 on page 48 of 8500.2.

and confidentiality in accordance with OMB Circular A-130 (reference (v)). (8500.2, page 20) [4]

The IACs are presented in six Attachments (A1, A2, …, A6) to Enclosure 4 of 8500.2, extending from page 54 to the end of the document on page 102. There are 298 IACs presented in these attachments. Many of the IACs appear multiple times in the attachments. In order to distinguish these multiple appearances from each other, this report gives each appearance an "index," from 1 to 298, which is the IAC's order of appearance. For ease of reference the notation "IAC:1" refers to the first IAC, "IAC:2" refers to the second, and so on. In this way the three appearances of IAC COBR-1, for example, can be distinguished as follows: IAC:58, IAC:128, and IAC:192.

Each IAC is in one of eight subject areas and each subject area has its own abbreviation, as shown in the following table, reproduced from 8500.2.[5]

Table 2 Subject Areas

Abbreviation	Subject Area Name	Number of Controls in Subject Area
EC	Enclave and Computing Environment	48
DC	Security Design & Configuration	31
PE	Physical and Environmental	27
CO	Continuity	24
EB	Enclave Boundary Defense	8
IA	Identification and Authentication	9
PR	Personnel	7
VI	Vulnerability and Incident Management	3
TOTAL		157[6]

To simplify references to IA Control Numbers, this report uses the abbreviation "IACN."

The first two characters of an IACN are the abbreviation of the IAC's subject area. For example, we know that ECCT-1 is in the "Enclave and Computing Environment" subject area because the first two characters of the IACN are "EC," which is the abbreviation for that subject area.

---

[4] Another way to resolve this discrepancy would be to equate "control class" with "subject area" and to leave the set {management, personnel, operational, technical} unnamed. This alternate resolution is not used in this report because it would cause confusion when NIST 800-53 is considered later in this report: NIST 800-53 uses "class" to refer to the set {management, operational, technical}. Meanwhile, 8500.2 does not use either "control class" or the set {management, personnel, operational, technical} anywhere else except in the definition of "IA Control" so the resolution that this report uses creates no constraints elsewhere in the report.

[5] This is Table E4.T1 from page 49 of 8500.2, except that in this document a total is shown and the subject areas are listed in descending order of the number of IACs in the subject area, which is the same order used in this report.

[6] The cardinality of this set—157—is the same as the "IAC-Unique" set, presented later in this section.

With one exception, the IACs are listed in the attachments in alphabetical order within subject areas and the subject areas are listed in the order shown in the Table E4.T1 on page 49 of 8500.2, namely, DC, IA, EC, EB, PE, PR, CO, and VI. 8500.2 provides no explanation for this order. However, it seems to fit a lifecycle:

1. First we design a system (DC),
2. which includes design for identification and authentication (IA);
3. we next consider the enclave where the system will reside (EC),
4. followed by consideration of the enclave boundary (EB);
5. as we install the system we consider the site and its environment (PE),
6. then the people who will run the system (PR);
7. we next consider how to keep the system operational and contingency plans for when it runs into problems (CO); and
8. finally we prepare for incidents and updates (VI).

Unfortunately there is no obvious benefit from this order of the subject areas and 8500.2 does not explain or exploit it. For example, 8500.2 does not recommend consideration of the IACs in DC before IA and in IA before EC or that the IACs in DC are more important than the ones in IA. Listing the subject areas alphabetically, on the other hand, would at least facilitate locating particular IACs in the attachments.[7] The one exception to this ordering is IAAC-1 that appears as IAC:233 and IAC:270 in Attachments A4 and A5, respectively. In both cases IAAC-1 appears outside of the IA group and between the IACs for EC and EB.[8] There is no explanation for this exception and no obvious benefit.

8500.2 divides all systems into nine "baseline IA levels" based on the Cartesian product of two parameters—"Mission Assurance Category" (MAC) and confidentiality level—each of which has a range of three values. The set of possible values for the MAC parameter is

{MAC I, MAC II, MAC III}

and the set of possible values for the confidentiality level parameter is

{Classified, Sensitive, Public}.

So the nine baseline IA levels are as follows:

1. MAC I Classified
2. MAC I Sensitive
3. MAC I Public

---

[7] By comparison, the controls in NIST 800-53 [10] are listed alphabetically by family, where "family" in 800-53 is similar to "subject area" in 8500.2.

[8] At least IAAC-1 is between subject areas and not within one.

4. MAC II Classified
5. MAC II Sensitive
6. MAC II Public

7. MAC III Classified
8. MAC III Sensitive
9. MAC III Public

The MAC parameter reflects differing needs for integrity & availability, where MAC I requires the highest need for integrity & availability and MAC III the lowest. The IACs for MAC I systems are found in Attachment A1 to 8500.2; the IACs for MAC II and III systems are found in Attachments A2 and A3, respectively.

The confidentiality level parameter reflects differing needs for confidentiality, where Classified requires the highest need for confidentiality and Public the lowest. The IACs for systems with a Classified confidentiality level are found in Attachment A4 to 8500.2; the IACs for systems with Sensitive and Public confidentiality levels are found in Attachments A5 and A6, respectively.

A given system is "assigned" a MAC and a confidentiality level by a process that is outside of the scope of 8500.2.

The set of assigned IACs for each of the nine baseline IA levels is the union of the IACs in the two, relevant attachments, as shown in the following table, reproduced from 8500.2.[9]

Table 3 Assigned IA Controls by Mission Assurance Category and Confidentiality Level

	Classified	**Sensitive**	**Public**
MAC I	A1 ∪ A4	A1 ∪ A5	A1 ∪ A6
MAC II	A2 ∪ A4	A2 ∪ A5	A2 ∪ A6
MAC III	A3 ∪ A4	A3 ∪ A5	A3 ∪ A6

The following table shows the number of IACs in each attachment and the index range for the IACs in that attachment.[10]

[9] This is Figure E4.T2 from page 50 of 8500.2 with three exceptions. The first exception is that the rendering in this report is different: the table in 8500.2 is a 10x2 matrix. The second exception is that an apparent mistake in the table in 8500.2 is corrected here: the Attachments for a MAC II Public system should be A2 and A6 but the table in 8500.2 shows them as A3 and A6. The third exception is that the table shows "Attachments A1 and A4," for example, whereas this table shows the more precise "A1 ∪ A4," where "∪" represents the union of sets A1 and A4.

[10] This table does not appear in 8500.2.

Table 4 Attachments and IACs

Attachment	IACs in the Attachment	IAC Index Range
A1	70	1-70
A2	70	71-140
A3	64	141-204
A4	45	205-249
A5	37	250-286
A6	12	287-298

The approximate number of IACs in each of the nine baseline IA levels is shown in the next table, where the formula in each cell shows the number of IACs in each of the two contributing attachments, as shown in the previous table.[11]

Table 5 IACs in Each Baseline IA level

	MAC I	MAC II	MAC III
Classified	70 + 45 = 115	70 + 45 = 115	64 + 45 = 109
Sensitive	70 + 37 = 107	70 + 37 = 107	64 + 37 = 101
Public	70 + 12 = 82	70 + 12 = 82	64 + 12 = 76

The advantage of the way that 8500.2 lists the IACs—i.e., by using attachments—is that it simplifies identification of the IACs for a given baseline IA level. In fact, the attachment approach makes it almost impossible to misidentify the IACs for a given baseline IA level: you just print a copy of 8500.2, retain the pages for the relevant attachments, and discard the rest. This is a decisive advantage. The disadvantage of the attachment approach is that IACs can appear more than once across the attachments.

An alternative way of listing the IACs would be in a 157x9 table, one row for each IAC and one column for each baseline IA level. An "x" in cell (m,n) would indicate that the mth IAC applies to the nth baseline IA level. The table approach would eliminate duplicates but it would make it problematic to identify the IACs for a given baseline IA level. In fact, the table approach would make it almost impossible to identify reliably and consistently the IACs for a given baseline IA level, so easy would it be to get confused about rows and columns and which IACs are to be chosen and which are to be left behind.[12]

---

[11] This table does not appear in 8500.2. The totals in the table are approximate because no accounting is made for duplicates across attachments. For example, DCSS-2 appears in both Attachments A1 and A4, so the number of IACs for MAC I Classified systems is at least one less than the sum of the number of IACs in Attachments A1 and A4.

[12] Jumping ahead in the report, a third listing scheme would be to gather all the IACs that apply to all of the baseline IA levels—as the reader will discover these are the 43 Type 3 IACs—and move them all to a new attachment, call it Attachment 0. This would reduce the duplication of IACs, reducing the total appearances by two for each Type 3 IAC. So instead of 298 appearances we would have 298 – (2*43) = 212. The user would then retain the pages for three attachments: (1) Attachment 0; (2) one of Attachments 1, 2, or 3; and (3) one of Attachments 4, 5, or 6.

The trailing dash and integer in an IACN is the IAC's "control level" and it specifies one of three "robustness" levels—1, 2, or 3, where 1 is the lowest and 3 is the highest. So, for example, we have CODB-1, CODB-2, and CODB-3.

The IACs that differ only in their robustness are in the same "IA Control Group" (ICG), as this report calls it. The name of an ICG is the IACN of any IAC in the ICG but without the trailing control level. For example, the three IACs listed in the previous paragraph are all in ICG CODB. As we will see later in this section, there are 109 ICGs. (Note that in this report "ICG" can refer to any of the IACs in a given ICG, depending upon the context.)

By definition IACs in the same ICG have different robustness levels. The levels obey explicit[13] constraints that this report refers to as the "Robustness Rule"[14] which is as follows:

> All ICGs have an IAC with robustness 1 but only ICGs that have an IAC with robustness 2 have an IAC with robustness 3.

So, using ICG ECCT from Table 1 as an example,

- If we were to see ECCT-3 in an attachment this would imply that there is at least one ECCT-2 and at least one ECCT-1 somewhere in the collection of attachments.
- If we were to see ECCT-2 in an attachment this would imply that there is at least one ECCT-1 somewhere in the collection of attachments but this does not imply that an ECCT-3 exists in any attachment.
- We will certainly see ECCT-1 in some attachment but this does not imply that either an ECCT-3 or an ECCT-2 exist in any attachment.

In general, the IA Control Text for IACs with different robustness levels in the same ICG is cumulative. That is, the IA Control Text for the IAC with the robustness level of 3 is a proper superset of the IA Control Text for the IAC with the robustness level of 2 and similarly for the IA Control Texts for the IACs with the robustness levels of 2 and 1.[15] For example,

- the IA Control Text for ECAR-1 lists four items that are to be included in audit records;
- the IA Control Text for ECAR-2 adds five items to the list for ECAR-1; and
- the IA Control Text for ECAR-3 adds four items to the list for ECAR-2.

Where concentricity of IA Control Text cannot be accommodated, robustness reflects rigor instead. For example,

---

[13] See Paragraph E4.1.3.4 on page 49 of 8500.2.

[14] 8500.2 does not provide a name for these constraints but because this report needs to refer to these constraints elsewhere a name is provided for them here.

[15] For IACs in the same ICG, the IA Control Name is the same, with only minor exceptions (such as for DCSR), and the subject area of course is the always the same.

- the IA Control Text for ECCR-1 concerns sensitive information;
- the IA Control Text for ECCR-2 concerns classified, non-SAMI information; and
- the IA Control Text for ECCR-3 concerns all SAMI information.

One would expect that multiple appearances of a given IACN would have the same IA Control Text. It should be a simple matter of cut & paste. But surprisingly this is not the case. While the meaning is always consistent across multiple appearances of a given IACN, the text is not. For example, DCCS-2 has two appearances: IAC:4 and IAC:74. The last sentence of IAC:4 is

> If a DoD reference document is not available, the system owner works with DISA or NSA to draft configuration guidance for inclusion in a Department reference guide. (8500.2, page 54)

but the last sentence of IAC:74 is

> If a Departmental reference document is not available, the system owner works with DISA or NSA to draft configuration guidance for inclusion in a DoD reference guide. (8500.2, page 65)

If the DoD is the department to which "Departmental" refers, then the meaning is the same.

ECND-2 has two appearances. IAC:32 shows

> …solutions (e.g., IAVA)… (8500.2, page 59)

but IAC:102 shows

> …solutions, e.g., IAVA… (8500.2, page 70).

EBRU-1 has two appearances. IAC:236 shows

> …session-level… (8500.2, page 91)

but IAC:274 shows

> …session level… (8500.2, page 98).

DCID-1 has three appearances. IAC:9 and IAC:79 both show

> …(potential)… (8500.2, pages 55 & 66)

but IAC:149 shows

> …[potential]… (8500.2, page 77).

DCSD-1 also has three appearances. IAC:19 and IAC:157 both show

…roles (e.g., DAA and IAM/IAO) are… (8500.2, pages 57 & 79)

but IAC:89, shows

…roles, e.g., DAA and IAM/IAO, are… (8500.2, page 68).

There are also differences in the shared text for IACNs of different robustness for the same IAC. For example, DCCB-1's only appearance (IAC:143) refers to the

…configuration control board… (8500.2, page 76)

but both of DCCB-2's appearances (IAC:3 & IAC:73) refer to the

…Configuration Control Board… (8500.2, pages 54 & 65).

ECND-1's only appearance, IAC:167, shows

…device (e.g., routers, switches, firewalls) control program is… (8500.2, page 80)

but both appearances of ECND-2 (IAC:32 and IAC:102) show

…device control program (e.g., routers, switches, firewalls) is… (8500.2, pages 59 & 70).

It is difficult to account for these differences. Are they watermarks? But if so, for what purpose would they serve? It seems more likely that they are the result of changes when the document was almost final.[16]

We can now revisit the material above and provide context by presenting three sets:

- "IAC-All" is the set of 298 IACs in the six attachments;
- "IAC-Unique" is the set of 157 unique IACs in IAC-All; and
- "ICG" is the set of 109 ICGs in IAC-Unique
    - or, equivalently, ICG is the set of ICGs corresponding to the IACs with robustness 1 in IAC-Unique.

The next table summarizes the names and contents of these sets.

Table 6 IA Control Sets

Set Name	Elements	Comments
IAC-All	298	This is the set of IACs as shown in the six attachments to 8500.2.
IAC-Unique	157	This is the set of unique IACs in IAC-All.
ICG	109	This is the set of ICGs in IAC-Unique.

[16] This suggests an editor function that we could call "synchronized copy:" making a change in one synchronized copy of passage X is automatically reflected in all other synchronized copies of passage X.

To confirm understanding of these three sets, consider the IACs in ICG ECMT:

- ECMT-2 appears in Attachment A4 (as IAC:225) and
- ECMT-1 appears in Attachments A5 (as IAC:264) and A6 (as IAC:292).

These IACs contribute

- three items to IAC-All (namely, IAC:225, IAC:264, and IAC:292),
- two items to IAC-Unique (namely, ECMT-2 and ECMT-1), and
- one item to ICG (namely, ECMT).

For ease of reference each ICG is given an "index" from 1 to 109. The ICG index is assigned based on the order of the ICG when the list is sorted alphabetically within "signature" within "type," both of which are explained in a subsequent section.

The next table lists the ICGs, along with their index ("#") and IA Control Name, sorted in ascending order of ICG index, as denoted by the highlighted column.

Table 7 ICGs, Sorted on ICG Index

#	ICG	IA Control Name
1	ECNK	Encryption for Need-To-Know
2	ECCR	Encryption for Confidentiality (Data at Rest)
3	ECCT	Encryption for Confidentiality (Data at Transmit)
4	ECLO	Logon
5	IAIA	Individual Identification and Authentication
6	PECF	Access to Computing Facilities
7	PECS	Clearing and Sanitizing
8	PEPF	Physical Protection of Facilities
9	PRAS	Access to Information
10	EBPW	Public WAN Connection
11	ECCM	COMSEC
12	ECLC	Audit of Security Label Changes
13	PEDD	Destruction
14	EBRP	Remote Access for Privileged Functions
15	EBRU	Remote Access for User Functions
16	ECAD	Affiliation Display
17	ECAN	Access for Need-to-Know
18	ECIC	Interconnections among DoD Systems and Enclaves
19	ECML	Marking and Labeling
20	ECRC	Resource Control
21	ECTC	Tempest Controls
22	IAAC	Account Control
23	IAGA	Group Authentication
24	PEDI	Data Interception
25	PEPS	Physical Security Testing

26	PESP	Workplace Security Procedures
27	PESS	Storage
28	PEVC	Visitor Control to Computing Facilities
29	PRTN	Information Assurance Training
30	DCPA	Partitioning the Application
31	DCPB	IA Program and Budget
32	DCSP	Security Support Structure Partitioning
33	ECDC	Data Change Controls
34	ECID	Host Based IDS
35	ECTB	Audit Trail Backup
36	ECMT	Conformance Monitoring and Testing
37	PRMP	Maintenance Personnel
38	DCSR	Specified Robustness – Basic
39	EBBD	Boundary Defense
40	ECAR	Audit Record Content
41	COEB	Enclave Boundary Defense
42	COED	Scheduled Exercises and Drills
43	COSP	Spares and Parts
44	VIIR	Incident Response Planning
45	COAS	Alternate Site Designation
46	COEF	Identification of Essential Functions
47	COMS	Maintenance Support
48	DCCB	Control Board
49	DCCS	Configuration Specifications
50	ECND	Network Device Controls
51	ECPC	Production Code Change Controls
52	ECSD	Software Development Change Controls
53	ECTM	Transmission Integrity Controls
54	IATS	Token and Certificate Standards
55	PEEL	Emergency Lighting
56	PEFD	Fire Detection
57	PEFS	Fire Suppression
58	PEHC	Humidity Controls
59	PETC	Temperature Controls
60	DCSS	System State Changes
61	ECCD	Changes to Data
62	ECAT	Audit Trail, Monitoring, Analysis and Reporting
63	IAKM	Key Management
64	CODB	Data Backup Procedures
65	CODP	Disaster and Recovery Planning
66	COPS	Power Supply
67	DCAS	Acquisition Standards
68	ECLP	Least Privilege
69	ECRR	Audit Record Retention
70	ECWM	Warning Message

71	PRNK	Access to Need-to-Know Information
72	COBR	Protection of Backup and Restoration Assets
73	COSW	Backup Copies of Critical SW
74	COTR	Trusted Recovery
75	DCAR	Procedural Review
76	DCBP	Best Security Practices
77	DCCT	Compliance Testing
78	DCDS	Dedicated IA Services
79	DCFA	Functional Architecture for AIS Applications
80	DCHW	HW Baseline
81	DCID	Interconnection Documentation
82	DCII	IA Impact Assessment
83	DCIT	IA for IT Services
84	DCMC	Mobile Code
85	DCNR	Non-repudiation
86	DCPD	Public Domain Software Controls
87	DCPP	Ports, Protocols, and Services
88	DCPR	CM Process
89	DCSD	IA Documentation
90	DCSL	System Library Management Controls
91	DCSQ	Software Quality
92	DCSW	SW Baseline
93	EBCR	Connection Rules
94	EBVC	VPN Controls
95	ECIM	Instant Messaging
96	ECPA	Privileged Account Control
97	ECRG	Audit Reduction and Report Generation
98	ECSC	Security Configuration Compliance
99	ECTP	Audit Trail Protection
100	ECVI	Voice-over-IP (VoIP) Protection
101	ECVP	Virus Protection
102	ECWN	Wireless Computing and Network
103	PEFI	Fire Inspection
104	PEMS	Master Power Switch
105	PESL	Screen Lock
106	PETN	Environmental Control Training
107	PEVR	Voltage Regulators
108	PRRB	Security Rules of Behavior or Acceptable Use Policy
109	VIVM	Vulnerability Management

For ease of reference, the index of an ICG is sometimes provided when referring to the ICG (e.g., “ICG #1 ECNK”).

The next table has the same contents as the previous table but is sorted alphabetically on ICG and thus provides an ICG-to-index translation.

Table 8 ICGs, Sorted Alphabetically on ICG

#	ICG	IA Control Name
45	COAS	Alternate Site Designation
72	COBR	Protection of Backup and Restoration Assets
64	CODB	Data Backup Procedures
65	CODP	Disaster and Recovery Planning
41	COEB	Enclave Boundary Defense
42	COED	Scheduled Exercises and Drills
46	COEF	Identification of Essential Functions
47	COMS	Maintenance Support
66	COPS	Power Supply
43	COSP	Spares and Parts
73	COSW	Backup Copies of Critical SW
74	COTR	Trusted Recovery
75	DCAR	Procedural Review
67	DCAS	Acquisition Standards
76	DCBP	Best Security Practices
48	DCCB	Control Board
49	DCCS	Configuration Specifications
77	DCCT	Compliance Testing
78	DCDS	Dedicated IA Services
79	DCFA	Functional Architecture for AIS Applications
80	DCHW	HW Baseline
81	DCID	Interconnection Documentation
82	DCII	IA Impact Assessment
83	DCIT	IA for IT Services
84	DCMC	Mobile Code
85	DCNR	Non-repudiation
30	DCPA	Partitioning the Application
31	DCPB	IA Program and Budget
86	DCPD	Public Domain Software Controls
87	DCPP	Ports, Protocols, and Services
88	DCPR	CM Process
89	DCSD	IA Documentation
90	DCSL	System Library Management Controls
32	DCSP	Security Support Structure Partitioning
91	DCSQ	Software Quality
38	DCSR	Specified Robustness - Basic
60	DCSS	System State Changes
92	DCSW	SW Baseline
39	EBBD	Boundary Defense
93	EBCR	Connection Rules

#	ICG	IA Control Name
10	EBPW	Public WAN Connection
14	EBRP	Remote Access for Privileged Functions
15	EBRU	Remote Access for User Functions
94	EBVC	VPN Controls
16	ECAD	Affiliation Display
17	ECAN	Access for Need-to-Know
40	ECAR	Audit Record Content
62	ECAT	Audit Trail, Monitoring, Analysis and Reporting
61	ECCD	Changes to Data
11	ECCM	COMSEC
2	ECCR	Encryption for Confidentiality (Data at Rest)
3	ECCT	Encryption for Confidentiality (Data at Transmit)
33	ECDC	Data Change Controls
18	ECIC	Interconnections among DoD Systems and Enclaves
34	ECID	Host Based IDS
95	ECIM	Instant Messaging
12	ECLC	Audit of Security Label Changes
4	ECLO	Logon
68	ECLP	Least Privilege
19	ECML	Marking and Labeling
36	ECMT	Conformance Monitoring and Testing
50	ECND	Network Device Controls
1	ECNK	Encryption for Need-To-Know
96	ECPA	Privileged Account Control
51	ECPC	Production Code Change Controls
20	ECRC	Resource Control
97	ECRG	Audit Reduction and Report Generation
69	ECRR	Audit Record Retention
98	ECSC	Security Configuration Compliance
52	ECSD	Software Development Change Controls
35	ECTB	Audit Trail Backup
21	ECTC	Tempest Controls
53	ECTM	Transmission Integrity Controls
99	ECTP	Audit Trail Protection
100	ECVI	Voice-over-IP (VoIP) Protection
101	ECVP	Virus Protection
70	ECWM	Warning Message
102	ECWN	Wireless Computing and Network
22	IAAC	Account Control
23	IAGA	Group Authentication
5	IAIA	Individual Identification and Authentication
63	IAKM	Key Management
54	IATS	Token and Certificate Standards
6	PECF	Access to Computing Facilities

#	ICG	IA Control Name
7	PECS	Clearing and Sanitizing
13	PEDD	Destruction
24	PEDI	Data Interception
55	PEEL	Emergency Lighting
56	PEFD	Fire Detection
103	PEFI	Fire Inspection
57	PEFS	Fire Suppression
58	PEHC	Humidity Controls
104	PEMS	Master Power Switch
8	PEPF	Physical Protection of Facilities
25	PEPS	Physical Security Testing
105	PESL	Screen Lock
26	PESP	Workplace Security Procedures
27	PESS	Storage
59	PETC	Temperature Controls
106	PETN	Environmental Control Training
28	PEVC	Visitor Control to Computing Facilities
107	PEVR	Voltage Regulators
9	PRAS	Access to Information
37	PRMP	Maintenance Personnel
71	PRNK	Access to Need-to-Know Information
108	PRRB	Security Rules of Behavior or Acceptable Use Policy
29	PRTN	Information Assurance Training
44	VIIR	Incident Response Planning
109	VIVM	Vulnerability Management[17]

Appendix B shows the 298 IACs in two tables, the first sorted on appearance index and the second sorted on attachment within IA Control Number.

With the above foundation material in hand we are ready to consider analysis of 8500.2.

[17] ICG VIVM just happens to be the last in both tables.

3 ANALYSIS OF IA CONTROLS

This section analyzes the IACs by partitioning the set of ICGs using the following seven partitions:[18]

- Type
- Span
- CIA (i.e., Confidentiality, Integrity, Availability)
- Impact
- Family
- Class
- Coverage.

Each partition is presented in a separate section below.

8500.2 divides up the IACs and ICGs in various ways and some but not all of these ways are used by the seven partitions shown above. The five "dividers," as we will call them, provided by 8500.2 are as follows[19]:

---

[18] A partition of a set S is a set of subsets, referred to in this report for ease of reference as "partition subsets," such that both of the following are true: (1) each element of S is in exactly one partition subset, and (2) the union of the partition subsets equals S. These two conditions together imply that the intersection of any two partition subsets is null.

[19] There are other possible partitions. One example is SPAWAR's {design, configurable, and physical/environmental} set for "IA Controls" ([11], page 21). (Presumably the set of IA Controls to which this SPAWAR document refers is the set that this report identifies as the IAC-Unique set but which, without loss of generality and for ease of analysis, we will assume in this footnote to be the ICG set.) The three subsets are described as follows:

> (1) the ICGs in the design subset are part of the "basic design" and are tested only once, in the laboratory;
>
> (2) the ICGs in the physical/environmental subset are "part of the physical environment into which a system is installed" and, like the ICGs in the design subset, are tested only once, but at the site; and
>
> (3) the ICGs in the configuration subset are "part of the basic design of a system, but depend upon proper configuration" so these ICGs are tested twice—at the laboratory and at the site.

Unfortunately the partitioning is equivocal. Consider, for example, COPS-2 (IAC:135), the IA Control Text for which reads "Electrical systems are configured to allow continuous or uninterrupted power to key IT assets. This may include an uninterrupted power supply coupled with emergency generators." The "basic design" must identify the "key IT assets;" this particular control "depends upon proper configuration;" and power is "part of the physical environment into which a system is installed." So this ICG could go into any of the three subsets. Although subset membership appears to be unequivocal for

- Subject Areas
- Robustness Levels
- CIA
- Attachments
- Baseline IA Levels.

The partition named "CIA" and the divider named "CIA" are identical but there is no corresponding equivalence between the other partitions and the other dividers.

The three sets that the above dividers could partition, introduced in the previous section, are as follows:

- IAC-All
- IAC-Unique
- ICG

The next bullets describe how the dividers partition or do not partition the three sets:

- The subject areas partition all three sets—IAC-All, IAC-Unique, and ICG—(because each member of each of those sets is in exactly one subject area).
- Robustness levels partition IAC-All and IAC-Unique (because each member of those sets has exactly one robustness level) but not ICG (because ICG #1 ECNK, for example, has two robustness levels—1 and 2).
- CIA partitions IAC-All and IAC-Unique (because each member of those sets is marked either Confidentiality or Integrity or Availability) but not ICG (because of the following one exception: ICG #40 ECAR has ECAR-3 (IAC:213) marked Integrity and ECAR-2 (IAC:256) and ECAR-1 (IAC:289), both marked Confidentiality).
- The Attachments partition IAC-All (because each member of IAC-All is in exactly one attachment) but not IAC-Unique (because ECNK-1, for example, is in more than one attachment, as IAC:226 in Attachment A4 and as IAC:265 in Attachment A5) and not ICG (because ICG #1 ECNK, for example, is in more than one attachment, namely Attachments A4 and A5).
- The baseline IA levels do not partition any of the three sets. The baseline IA levels do not partition IAC-All (because IAC:1 (which is DCAR-1), for example, is in all three MAC I baseline IA levels) and not IAC-Unique (because ECNK-1, for example, is in six baseline IA levels) and not ICG (because ICG #1 ECNK, for example, is in six baseline IA levels).

---

some ICGs—such as CODP, IAIA, and PETC—there are many other ICGs in the same equivocal state as COPS.

Unlike 8500.2's {management, personnel, operational, technical} partition, discussed in a previous footnote, the document from SPAWAR defines the names for and the purpose of these three subsets but, like 8500.2's {management, personnel, operational, technical} partition, the document from SPAWAR does not appear to tell us which ICGs belong in which subset, nor does the document from SPAWAR appear to indicate that there is no need to provide this, because, for example, such assignment needs to be done on a system-by-system basis.

The next table summarizes the above bullets.

Table 9 Candidate Partitions in 8500.2

Candidate Partition	Set		
	IAC-All	IAC-Unique	ICG
Subject Areas	X	X	X
Robustness Levels	X	X	
CIA	X	X	
Attachments	X		
Baseline IA Levels			

Of the five dividers only the subject area partitions all three sets. This divider is addressed in a separate section below.

At the end of each section below is a "partition table" that shows the value for each ICG for each of the seven partitions listed at the beginning of this section. In order to introduce the structure of that table, a fragment of the partition table is shown below. The meaning of the cell values is explained when the associated partition is presented.

Table 10 Partition Table, Sorted on Type (Fragment)

#	ICG	Signature	Type	CIA	Span	Impact	Family	Class	Coverage
1	ECNK	---1+21-	0	C	2	C	SC-9	T	DS5.11
2	ECCR	---2+31-	0	C	2	Z	SC-28	T	DS11.6
3	ECCT	---21-	0	C	2	B	SC-9	T	DS5.11
…									
109	VIVM	111---	3	A	1	C	RA-5	M	DS5.2

3.1 Type

This section explores the "type" partition, which is a function of an ICG's "signature." Signatures and types are presented in the first section below. The second section presents signature "patterns" and how the ICGs that do not follow them can or, in some cases, cannot be adjusted to follow them. The third and last section shows that the set of signatures in 8500.2 covers all allowable signatures, subject to the constraints imposed by the signature patterns and the Robustness Rule.

3.1.1 Signatures

A "signature" is represented in this document as an ordered 6-tuple that indicates presence in or absence from the six attachments (A1, A2,…,A6) to Enclosure 4 of 8500.2. If there is an IAC for a given ICG in the ith attachment, then the ith slot in the signature for that ICG is the robustness ("1," "2," or "3") of that IAC. If, on the other hand, there is no IAC for a given ICG in the ith attachment, then the ith slot in the signature for that ICG is a dash ("-").

For example, ICG #3 ECCT does not appear in Attachments A1, A2, A3, and A6 but it does appear as ECCT-2 in Attachment A4 and as ECCT-1 in Attachment A5, so the signature

- for ICG #3 ECCT is ---21-.

As a second example, ICG #30 DCPA does not appear in Attachments A3, A4, A5, and A6 but it does appear as DCPA-1 in Attachments A1 and A2, so the signature

- for ICG #30 DCPA is 11----.

As two additional examples, chosen somewhat at random, the signature

- for ICG #64 CODB is 321---, and
- for ICG #67 DCAS is ---111.

Signatures indicate the ICGs that are universal (i.e., they apply to all nine of the baseline IA levels defined in 8500.2). The signatures that correspond to universal ICGs have either an integer in at least all of the *first* three slots of the signature, in which case the ICG applies to any MAC Level, or an integer in at least all of the *last* three slots of the signature, in which case the ICG applies to any Confidentiality Level. The signatures shown above for CODB and DCAS fit this pattern, indicating that these two ICGs are universal, and the signatures for ECCT and DCPA do not, indicating that these two ICGs are not universal.

Signatures also indicate the ICGs that have constant robustness (i.e., they have an IAC with robustness 1 but no IAC for either robustness 2 or 3). These ICGs have no variants. The signatures shown above for DCPA and DCAS fit this pattern and the signatures for ECCT and CODB do not (because ECCT has two robustness levels (levels 1 and 2) and CODB has all three robustness levels (levels 1, 2, and 3)).

Combining these two patterns—universality and constant robustness—provides four types, as shown in the next table, that partition the ICG set.

Table 11 ICG Types

Type	ICG Universal? (i.e., ICG applies to all baseline IA levels)	Constant Robustness? (i.e., ICG has only one robustness level)	Number of ICGs of this Type	Percentage of All ICGs	Example Signature	Example ICG
0	No	No	9	8%	---21-	ECCT
1	No	Yes	26	24%	11----	DCPA
2	Yes	No	31	28%	321---	CODB
3	Yes	Yes	43	40%	---111	DCAS
TOTAL			109	100%		

The ICG types have the following characteristics:

- Type 3 ICGs apply to all baseline IA levels and have constant robustness.
- Type 2 ICGs apply to all baseline IA levels but they vary in robustness.
- Type 1 ICGs do not apply to all baseline IA levels but they have constant robustness.
- Type 0 ICGs do not apply to all baseline IA levels nor do they have constant robustness.

Type 3 ICGs form what we could call a base of ICGs within the core of the ICG set. Each of these appears only once in the IAC-Unique set, meaning that each IAC for these ICGs has robustness 1. All of these ICGs apply to all nine of the baseline IA levels. Type 2 ICGs also apply to all nine of the baseline IA levels but they vary in robustness. We could say then that there are 43 base IA Controls—the Type 3 ICGs—that apply just as they are to all systems and there are an additional 31 IA Controls—the Type 2 ICGs—that also apply to all systems but these vary in robustness. This leaves 35 ICGs—the Type 1 and Type 0 ICGs—that do not apply to all systems and/or vary in robustness.

The next table shows the appearance index in each attachment for each IAC, sorted in ascending alphabetical IACN order, along with the signature and type of the ICG. Note that the robustness of each appearance can be determined by the associated signature. Note also that the peculiar notation in ECNK's signature, ---1+2-, for example, indicates that both ECNK-1 and ECNK-2 appear in Attachment A4. To start the reader on this table, consider ICG #45 COAS, covering the first two rows in the table. COAS-1, with IAC-Unique index 1, has one appearance, as IAC:191 in Attachment A3. COAS-2, with IAC-Unique index 2, has two appearances, as IAC:57 in Attachment A1 and as IAC:127 in Attachment A2. ICG's signature is thus 221---, which puts the ICG in Type 2. (Note also that ECCM, ECLC, and PEDD are the only ICGs for which there is only one IAC (and they all appear in Attachment 4).)

Table 12 IAC-Unique Appearances and ICG Signatures & Types

IAC-Unique	ICG	IACN	Attachment						Signature	Type
			A1	A2	A3	A4	A5	A6		
1	45	COAS-1			191				221---	2
2		COAS-2	57	127						
3	72	COBR-1	58	128	192				111---	3
4	64	CODB-1			193				321---	2
5		CODB-2		129						
6		CODB-3	59							
7	65	CODP-1			194				321---	2
8		CODP-2		130						
9		CODP-3	60							
10	41	COEB-1		131	195				211---	2
11		COEB-2	61							
12	42	COED-1		132	196				211---	2
13		COED-2	62							
14	46	COEF-1			197				221---	2
15		COEF-2	63	133						
16	47	COMS-1			198				221---	2
17		COMS-2	64	134						
18	66	COPS-1			199				321---	2
19		COPS-2		135						
20		COPS-3	65							
21	43	COSP-1		136	200				211---	2
22		COSP-2	66							
23	73	COSW-1	67	137	201				111---	3
24	74	COTR-1	68	138	202				111---	3
25	75	DCAR-1	1	71	141				111---	3
26	67	DCAS-1				205	250	287	---111	3
27	76	DCBP-1	2	72	142				111---	3
28	48	DCCB-1			143				221---	2
29		DCCB-2	3	73						
30	49	DCCS-1			144				221---	2
31		DCCS-2	4	74						
32	77	DCCT-1	5	75	145				111---	3
33	78	DCDS-1	6	76	146				111---	3
34	79	DCFA-1	7	77	147				111---	3
35	80	DCHW-1	8	78	148				111---	3
36	81	DCID-1	9	79	149				111---	3
37	82	DCII-1	10	80	150				111---	3
38	83	DCIT-1	11	81	151				111---	3
39	84	DCMC-1	12	82	152				111---	3
40	85	DCNR-1	13	83	153				111---	3
41	30	DCPA-1	14	84					11----	1
42	31	DCPB-1	15	85					11----	1

IAC-Unique	ICG	IACN	Attachment						Signature	Type
			A1	A2	A3	A4	A5	A6		
43	86	DCPD-1	16	86	154				111---	3
44	87	DCPP-1	17	87	155				111---	3
45	88	DCPR-1	18	88	156				111---	3
46	89	DCSD-1	19	89	157				111---	3
47	90	DCSL-1	20	90	158				111---	3
48	32	DCSP-1	21	91					11----	1
49	91	DCSQ-1	22	92	159				111---	3
50	38	DCSR-1						288	---321	2
51		DCSR-2					251			
52		DCSR-3				206				
53	60	DCSS-1			160				2212--	2
54		DCSS-2	23	93		207				
55	92	DCSW-1	24	94	161				111---	3
56	39	EBBD-1						295	---321	2
57		EBBD-2					271			
58		EBBD-3				234				
59	93	EBCR-1	44	114	178				111---	3
60	10	EBPW-1					272	296	----11	1
61	14	EBRP-1				235	273		---11-	1
62	15	EBRU-1				236	274		---11-	1
63	94	EBVC-1	45	115	179				111---	3
64	16	ECAD-1				211	254		---11-	1
65	17	ECAN-1				212	255		---11-	1
66	40	ECAR-1						289	---321	2
67		ECAR-2					256			
68		ECAR-3				213				
69	62	ECAT-1			164		257	290	221211	2
70		ECAT-2	27	97		214				
71	61	ECCD-1			165				2212--	2
72		ECCD-2	28	98		215				
73	11	ECCM-1				216			---1--	1
74	2	ECCR-1					258		---2+31-	0
75		ECCR-2				217				
76		ECCR-3				218				
77	3	ECCT-1					259		---21-	0
78		ECCT-2				219				
79	33	ECDC-1	29	99					11----	1
80	18	ECIC-1				220	260		---11-	1
81	34	ECID-1	30	100					11----	1
82	95	ECIM-1	31	101	166				111---	3
83	12	ECLC-1				221			---1--	1
84	4	ECLO-1					261		---21-	0
85		ECLO-2				222				

IAC-Unique	ICG	IACN	Attachment						Signature	Type
			A1	A2	A3	A4	A5	A6		
86	68	ECLP-1				223	262	291	---111	3
87	19	ECML-1				224	263		---11-	1
88	36	ECMT-1					264	292	---211	2
89		ECMT-2				225				
90	50	ECND-1			167				221---	2
91		ECND-2	32	102						
92	1	ECNK-1				226	265		---1+21-	0
93		ECNK-2				227				
94	96	ECPA-1	33	103	168				111---	3
95	51	ECPC-1			169				221---	2
96		ECPC-2	34	104						
97	20	ECRC-1				228	266		---11-	1
98	97	ECRG-1	35	105	170				111---	3
99	69	ECRR-1				229	267	293	---111	3
100	98	ECSC-1	36	106	171				111---	3
101	52	ECSD-1			172				221---	2
102		ECSD-2	37	107						
103	35	ECTB-1	38	108		230			11-1--	1
104	21	ECTC-1				231	268		---11-	1
105	53	ECTM-1			173				221---	2
106		ECTM-2	39	109						
107	99	ECTP-1	40	110	174				111---	3
108	100	ECVI-1	41	111	175				111---	3
109	101	ECVP-1	42	112	176				111---	3
110	70	ECWM-1				232	269	294	---111	3
111	102	ECWN-1	43	113	177				111---	3
112	22	IAAC-1				233	270		---11-	1
113	23	IAGA-1				208	252		---11-	1
114	5	IAIA-1					253		---21-	0
115		IAIA-2				209				
116	63	IAKM-1			162				2213--	2
117		IAKM-2	25	95						
118		IAKM-3				210				
119	54	IATS-1			163				221---	2
120		IATS-2	26	96						
121	6	PECF-1					275		---21-	0
122		PECF-2				237				
123	7	PECS-1					276		---21-	0
124		PECS-2				238				
125	13	PEDD-1				239			---1--	1
126	24	PEDI-1				240	277		---11-	1
127	55	PEEL-1			180				221---	2
128		PEEL-2	46	116						

IAC-Unique	ICG	IACN	Attachment						Signature	Type
			A1	A2	A3	A4	A5	A6		
129	56	PEFD-1			181				221---	2
130		PEFD-2	47	117						
131	103	PEFI-1	48	118	182				111---	3
132	57	PEFS-1			183				221---	2
133		PEFS-2	49	119						
134	58	PEHC-1			184				221---	2
135		PEHC-2	50	120						
136	104	PEMS-1	51	121	185				111---	3
137	8	PEPF-1					278		---21-	0
138		PEPF-2				241				
139	25	PEPS-1				242	279		---11-	1
140	105	PESL-1	52	122	186				111---	3
141	26	PESP-1				243	280		---11-	1
142	27	PESS-1				244	281		---11-	1
143	59	PETC-1			187				221---	2
144		PETC-2	53	123						
145	106	PETN-1	54	124	188				111---	3
146	28	PEVC-1				245	282		---11-	1
147	107	PEVR-1	55	125	189				111---	3
148	9	PRAS-1					283		---21-	0
149		PRAS-2				246				
150	37	PRMP-1					284	297	---211	2
151		PRMP-2				247				
152	71	PRNK-1				248	285	298	---111	3
153	108	PRRB-1	56	126	190				111---	3
154	29	PRTN-1				249	286		---11-	1
155	44	VIIR-1		139	203				211---	2
156		VIIR-2	69							
157	109	VIVM-1	70	140	204				111---	3

3.1.2 Signature Patterns

With eight exceptions, all of the ICGs follow three patterns:

- Pattern 0:

  A given ICG appears at most once in any given Attachment.

- Pattern 1:

  If an ICG appears in Attachment A3, then it appears in Attachment A2 as well, and if an ICG appears in Attachment A2, then it appears in Attachment A1 as well.

Similarly, if an ICG appears in Attachment A6, then it appears in Attachment A5 as well, and if an ICG appears in Attachment A5, then it appears in Attachment A4 as well.

(This pattern reflects the ordering of importance of IACs for an ICG. If the ICG concerns integrity or availability, then there should always be an IAC for MAC I systems. If there is an IAC for MAC I systems, then perhaps there is also an IAC for MAC II systems, and if there is an IAC for MAC II systems, then perhaps there is an IAC for MAC III systems. The same ordering is true for ICGs for Classified, Sensitive, and Public systems.)

- Pattern 2:

  A given ICG that appears in Attachments A1 and/or A2 and/or A3 does not also appear in Attachments A4 and/or A5 and/or A6, and the converse. That is, an ICG appears in one set of attachments or the other: it does not appear in both sets.

  (This pattern reflects the separation of ICGs into those designed for integrity or availability from those designed for confidentiality. ICGs are designed for only one of the three.)

(A fourth pattern is introduced in a subsequent section.)

The three patterns described above are not rich enough to cover all of the ICGs. Of the 109 ICGs, eight do not conform to these patterns, as noted above. Non-conformance to Pattern 0 is due to the way the IA Control Text is divided between the IACs of different robustness for the particular ICG. For these ICGs, this non-conformance is cosmetic and can be removed. But non-conformance to Patterns 1 and 2 cannot be removed without adding new ICGs that would be both awkward and confusing. The three patterns described above are descriptive, not prescriptive, so any changes to the ICGs in order to remove pattern non-conformance would be Procrustean. This discussion is intended only to deepen understanding of the ICGs. (The discussion also identifies two of ECAT's IACNs as superfluous, as we will see below.)

The eight ICGs that do not conform to these patterns are shown in the next table, sorted in ascending order of signature. Each pattern is discussed in a separate section below. (It is just coincidence that the contents of the "Pattern" and "Type" columns are the same.)

Table 13 Non-Conforming ICGs

#	ICG	Pattern	Signature	Type
1	ECNK	0	---1+21-	0
2	ECCR		---2+31-	
10	EBPW	1	----11	1
35	ECTB	2	11-1--	2
60	DCSS		2212--	
61	ECCD			

#	ICG	Pattern	Signature	Type
62	ECAT		221211 (equivalently 2212--)	
63	IAKM		2213--	

3.1.2.1 Pattern 0

For the two ICGs that do not conform to Pattern 0, namely ECNK and ECCR, the IACs can be adjusted so that the ICG conforms to the pattern. ECNK's signature is ---1+21-. If the IA Control Text of ECNK-2 were changed to incorporate much of the IA Control Text of ECNK-1, as shown below, then ECNK-1 would not need to appear in Attachment A4 and the signature would change to ---21-, allowing the ICG to conform to the pattern. The following is the IA Control Text of ECNK-1:

> Information in transit through a network at the same classification level, but which must be separated for need-to-know reasons is encrypted, at a minimum with NIST-certified cryptography. This is in addition to ECCT (encryption for confidentiality - data in transit).

And the following is the IA Control Text of ECNK-2:

> SAMI information in transit through a network at the same classification level is encrypted using NIST-certified cryptography. This is to separate it for need-to-know reasons. This is in addition to ECCT (encryption for confidentiality - data in transit).

If, as suggested above, ECNK-2 were to incorporate ECNK-1, then the following could be the IA Control Text of ECNK-2:

> Information in transit through a network at the same classification level, but which must be separated for need-to-know reasons is encrypted, at a minimum with NIST-certified cryptography. SAMI information in transit through a network at the same classification level is encrypted using NIST-certified cryptography to separate it for need-to-know reasons. This is in addition to ECCT (encryption for confidentiality - data in transit).

The situation for ECCR is almost the same as ECNK except that changing ECCR's IACs so that its signature, which is ---2+31-, changes to ---31- is not allowed because it breaks the Robustness Rule: an IAC with robustness of 3 implies the existence of an IAC for the same ICG with robustness of 2 (and an additional IAC for the same ICG with robustness 1). So the IACs in this case must be changed so that the signature becomes ---21-. This would require incorporating the IA Control Text for ECCR-3 into the IA Control Text for ECCR-2.

3.1.2.2 Pattern 1

EBPW, with signature ----11, is the only ICG that does not conform to Pattern 1. EBPW does not conform because the ICG does not appear in Attachment A4. We could create an EBPW-2, a new member of IAC-Unique, and put it in Attachment A4, thereby changing EBPW's signature to ---211 and bringing it into conformance with Pattern 1 but then we would have to write IA

Control Text for EPBW-2 which would need to be more robust than EBPW-1 and yet be the equivalent of a no-op. This may not be possible but it is almost certain to be confusing, which is too high a price to pay for conformance.

3.1.2.3 Pattern 2

All of the ICGs with signatures that do not conform to Pattern 2 do so because the ICG has a need for an increase in the robustness of classified systems alone. Conformance could be achieved by dividing the ICG, as will be shown below. But this is awkward and would increase confusion.

One of the ICGs that does not conform to Pattern 2 is ECTB, with signature 11-1--. The robustness levels for the nine baseline IA levels for signature 11-1-- are shown in the next table, using the assumption that the highest robustness level is chosen when there is a choice. The one cell that differs from signature 11---- (which signature conforms to all of the patterns) is shown highlighted.

Table 14 Robustness Levels for Signature 11-1--

	MAC I	MAC II	MAC III
Classified	1	1	1
Sensitive	1	1	-
Public	1	1	-

The highlighted cell indicates that for ECTB, MAC III Classified is different than MAC III Sensitive or Public. If a new ICG were created with signature ---1-- and if ECTB's signature were altered to 11----, then both ICGs would conform to all of the patterns. The new ICG would need to have the same IA Control Text as ECTB-1 but it would be in a different ICG, which would cause confusion.

ECAT is another ICG that does not conform to Pattern 2. ECAT's signature is 221211. This signature is equivalent to the simpler signature 2212--, as is shown in the next table, given the same assumption as used in the previous table, namely that the highest robustness level is chosen when there is a choice.

Table 15 Robustness Levels for Equivalent Signatures 221211 and 2212--

	MAC I	MAC II	MAC III
Classified	2	2	2
Sensitive	2	2	1
Public	2	2	1

The equivalence of ECAT's signature of 221211 to the simpler signature 2212-- implies that two of ECAT's IACs are superfluous. The following are ECAT's IACs:

- Attachment 1: IAC: 27 (ECAT-2)
- Attachment 2: IAC: 97 (ECAT-2)
- Attachment 3: IAC: 164 (ECAT-1)

- Attachment 4: IAC: 214 (ECAT-2)
- Attachment 5: IAC: 257 (ECAT-1)
- Attachment 6: IAC: 290 (ECAT-1)

Note that IAC:164 provides an IAC in all three MAC III baseline IA levels,[20] in which case IAC:257 and IAC:290 are superfluous: they are both taken care of by IAC:164, even though the value in the MAC III Classified cell is overridden by IAC:214.

Meanwhile, ICGs DCSS and ECCD have the same signature as ECAT's simpler signature, and all three of these ICGs can be made to conform to Pattern 2 in the same confusing way as ECTB, except that in all three cases the signature of the new ICG, ---2--, breaks the Robustness Rule.

IAKM is the last ICG that does not conform to Pattern 2. The robustness levels for IAKM's signature of 2213-- are shown in the next table, with the three cells that differ from signature 221--- (which signature conforms to all of the patterns) shown highlighted.

Table 16 Robustness Levels for Signature 2213--

	MAC I	MAC II	MAC III
Classified	3	3	3
Sensitive	2	2	1
Public	2	2	1

If for IAKM we were to follow the approach that we followed for the other ICGs that do not conform to Pattern 2, as described above, we would create a new ICG, call it IAKN, with signature ---3--, and we would change IAKM's signature to 221---. IAKM's signature now conforms to all of the patterns but IAKN's signature creates the same problem that this approach created with the other ICGs that do not conform to Pattern 2: the signature breaks the Robustness Rule. We can take care of this problem by changing IAKN's signature to ---1--. But this raises a new problem. The IA Control Text for what we are calling IAKN will be the IA Control Text IAKM-3, which is like IAKM-2 but of higher robustness. This leaves us with two ICGs that present two confusions. First, these two ICGs have IACs with IA Control Text so similar that they should be the same ICG. Second, the IA Control Text for IAKN's IAC with robustness 1 is more robust than IAKM's IAC of robustness 2. This is conformance at too high a price.

The next table summarizes the discussion above.

[20] That is, MAC III Classified, MAC III Sensitive, and MAC III Public.

Table 17 Non-Conforming ICGs (Summary)

ICG	Pattern	Signature	Type	Change to Achieve Conformance	
				New Signature	Signature of Additional ICG
ECNK	0	---1+21-	0	---21-	
ECCR		---2+31-		---21-	
EBPW	1	----11	1		
ECTB	2	11-1--	2	11----	---1--
DCSS		2212--		221---	---2--
ECCD		2212--			
ECAT		221211 (equivalently 2212--)			
IAKM		2213--			---1--

3.1.3 Allowable Signatures

This section shows that the set of signatures provided by the ICGs that follow the signature patterns described above cover the set of what we will call the "allowable" signatures.

Recall that a signature is represented in this document as an ordered 6-tuple that indicates presence in or absence from the six attachments (A1, A2,…,A6) to Enclosure 4 of 8500.2. If there is an IAC for a given ICG in the ith attachment, then the ith slot in the signature for that ICG is the robustness ("1," "2," or "3") of that IAC. If, on the other hand, there is no IAC for a given ICG in the ith attachment, then the ith slot in the signature for that ICG is a dash. There are thus $4^6 = 2^{12} = 4096$ such 6-tuples in the set of what we will call the "possible" signatures. (Note that this enumeration implicitly follows Pattern 0 which removes from consideration signatures, such as ECNK's and ECCR's, that represent more than one appearance of an ICG in any given attachment.)

The set of allowable signatures as we define it in this section is a proper subset of the set of possible signatures. The constraints that define that subset are (a) signature Patterns 1 and 2 described above, (b) a new pattern, Pattern 3, introduced in this section, and (c) the Robustness Rule, also described above.

Note first of all that the null signature, ------, is not an allowable signature because it represents an ICG that does not appear in any Attachment and thus needs no signature. So our set of allowable signatures begins with 4096 – 1 = 4095 elements.

Pattern 2 allows us to constrain consideration here to "half" signatures: we need to consider only three integers and/or dashes instead of the full six. This reduces the set of allowable signatures to $4^3 = 2^6 = 64$ elements, and we need to remove the null half signature, ---. This reduces the set to 64 - 1 = 63 elements.

Pattern 1 constrains the half signatures to be of three forms:

1. x--
2. xy-

3. xyz

where x, y, and z are integers in the set {1, 2, 3}.

As we will see in the table below,

- the x-- form generates 3 signatures;
- the xy- form generates 9 signatures; and
- the xyz form generates 27 signatures.

This reduces the set to 3 + 9 + 27 = 39 items.

We now introduce an additional signature pattern:

- Pattern 3:

  The robustness levels of the IACs for a given ICG that appear in Attachments A1, A2, and A3 (or Attachments A4, A5, and A6) must be monotonically decreasing. That is, the robustness level of the ICG's IAC that appears in Attachment A1 is at least as high as the robustness level of the corresponding IAC that appears in Attachment A2, and similarly for A2 and A3 (and similarly for A4, A5, and A6).

Pattern 3 constrains the set of allowable half signatures,

all of which are of the general form

abc

where

a, b, and c are in the set {1, 2, 3, -}

and

3 > 2 > 1 > -

to those half signatures for which

a >= b >= c.

The next table shows the 39 half signatures and identifies which are constrained by Pattern 3 and/or the Robustness Rule. The half signatures that are not constrained are highlighted.

Table 18 Allowable Half Signatures

	Half Signatures	Constrained by	
		Pattern 3	Robustness Rule
1	1--		
2	2--		X
3	3--		X
4	11-		
5	12-	X	
6	13-	X	X
7	21-		
8	22-		X
9	23-	X	X
10	31-		X
11	32-		X
12	33-		X
13	111		
14	112	X	
15	113	X	X
16	121	X	
17	122	X	
18	123	X	
19	131	X	X
20	132	X	
21	133	X	X
22	211		
23	212	X	
24	213	X	
25	221		
26	222		X
27	223	X	X
28	231	X	
29	232	X	X
30	233	X	X
31	311		X
32	312	X	
33	313	X	X
34	321		
35	322		X
36	323	X	X
37	331		X
38	332		X
39	333		X

We have now arrived at the set of allowable signatures, which consists of the following seven half signatures:

1. 1--
2. 11-
3. 21-
4. 111
5. 211
6. 221
7. 321

Note that by necessity

- any full signatures that match the 111 half signature will be of Type 3,
- any full signatures that match the 211, 221, or 321 half signatures will be of Type 2,
- any full signatures that match the 11- or 1-- half signatures will be of Type 1, and
- any full signatures that match the 21- half signature will be of Type 0, as shown in the next table.

Table 19 Half Signatures (and Types)

Half Signature	Type
111	3
211	2
221	
321	
1--	1
11-	
21-	0

The next table shows that neither the set of what we call "left signatures" (i.e., signatures that end with ---) nor the set of "right signatures" (i.e., signatures that begin with ---) alone cover the seven allowable signatures but together they do. This provides a sense of completeness. (The table shows, for each half signature, a sample ICG (along with the ICG's signature (which would be called a "full" signature in this context) and its type) from the set of left signatures and the set of right signatures.)

Table 20 Coverage of Allowable Signatures

Half Signature	Left Signature			Right Signature		
	Sample ICG	ICG Signature	ICG Type	Sample ICG	ICG Signature	ICG Type
1--				ECCM	---1--	1
11-	DCPA	11----	1	EBRP	---11-	
21-				ECCT	---21-	0
111	COBR	111---	3	DCAS	---111	3
211	COEB	211---	2	ECMT	---211	2
221	COAS	221---				
321	CODB	321---		DCSR	---321	2

3.1.4 Partition Table

The partition table, sorted on Type, is shown below.

Table 21 Partition Table, Sorted on Type

#	ICG	Signature	Type	CIA	Span	Impact	Family	Class	Coverage
1	ECNK	---1+21-	0	C	2	C	SC-9	T	DS5.11
2	ECCR	---2+31-	0	C	2	Z	SC-28	T	DS11.6
3	ECCT	---21-	0	C	2	B	SC-9	T	DS5.11
4	ECLO	---21-	0	C	2	C	AC-7	T	DS5.4
5	IAIA	---21-	0	C	2	A	IA-5	T	DS5.4
6	PECF	---21-	0	C	2	A	PE-2	O	DS12.3
7	PECS	---21-	0	C	2	A	MP-6	O	DS5.11
8	PEPF	---21-	0	C	2	A	PE-3	O	DS12.3
9	PRAS	---21-	0	C	2	A	PS-3	O	DS5.4
10	EBPW	----11	1	C	1	A	SC-7	T	DS5.10
11	ECCM	---1--	1	C	1	A	SC-12	T	DS5.8
12	ECLC	---1--	1	C	1	E	AU-3	T	DS5.5
13	PEDD	---1--	1	C	1	A	MP-6	O	DS11.4
14	EBRP	---11-	1	C	1	A	AC-17	T	DS5.10
15	EBRU	---11-	1	C	1	A	AC-17	T	DS5.10
16	ECAD	---11-	1	C	1	C	AC-3	T	DS5.3
17	ECAN	---11-	1	C	1	A	AC-3	T	DS5.4
18	ECIC	---11-	1	C	1	C	AC-4	T	DS5.10
19	ECML	---11-	1	C	1	A	MP-3	O	DS11.6
20	ECRC	---11-	1	C	1	C	SC-4	T	DS11.6
21	ECTC	---11-	1	C	1	A	PE-19	O	DS5.5
22	IAAC	---11-	1	C	1	A	AC-2	T	DS5.4
23	IAGA	---11-	1	C	1	C	IA-2	T	DS5.4
24	PEDI	---11-	1	C	1	A	PE-5	O	DS11.6
25	PEPS	---11-	1	C	1	E	PE-3	O	DS12.2
26	PESP	---11-	1	C	1	C	PL-4	M	DS11.6
27	PESS	---11-	1	C	1	A	MP-4	O	DS11.2
28	PEVC	---11-	1	C	1	A	PE-7+8	O	DS12.3
29	PRTN	---11-	1	I	1	A	AT-3	O	DS7.2
30	DCPA	11----	1	I	1	E	SC-2	T	DS11.6
31	DCPB	11----	1	A	1	A	SA-2	M	PO5.1
32	DCSP	11----	1	I	1	C	SC-3	T	DS5.7
33	ECDC	11----	1	I	1	C	CP-10	O	DS11.6
34	ECID	11----	1	I	1	C	SI-4	O	DS5.9
35	ECTB	11-1--	1	I	1	C	AU-9	T	DS11.5
36	ECMT	---211	2	C	2	D	CA-7	M	ME2.4
37	PRMP	---211	2	C	2	A	MA-5	O	DS1.3
38	DCSR	---321	2	C	3	A	SA-14	M	DS5.2
39	EBBD	---321	2	C	3	Z	SC-7	T	DS5.10

#	ICG	Signature	Type	CIA	Span	Impact	Family	Class	Coverage
40	ECAR	---321	2	ICC	3	Z	AU-3	T	DS5.5
41	COEB	211---	2	A	2	B	PE-17	O	DS4.2
42	COED	211---	2	A	2	D	CP-4	O	DS4.5
43	COSP	211---	2	A	2	D	MA-6	O	DS1.3
44	VIIR	211---	2	A	2	B	IR-8	O	DS8
45	COAS	221---	2	A	2	B	CP-7	O	DS4.2
46	COEF	221---	2	A	2	D	CP-2	O	DS4.2
47	COMS	221---	2	A	2	D	MA-6	O	DS1.3
48	DCCB	221---	2	I	2	D	CM-3	O	DS9
49	DCCS	221---	2	I	2	A	CM-6	O	DS9.1
50	ECND	221---	2	I	2	D	SC-7	T	DS5.10
51	ECPC	221---	2	I	2	C	AC-2	T	DS5.4
52	ECSD	221---	2	I	2	B	CM-5	O	DS11.3
53	ECTM	221---	2	I	2	C	SC-8	T	DS5.11
54	IATS	221---	2	I	2	C	IA-5	T	DS5.8
55	PEEL	221---	2	A	2	D	PE-12	O	DS12.4
56	PEFD	221---	2	A	2	A	PE-13	O	DS12.4
57	PEFS	221---	2	A	2	B	PE-13	O	DS12.4
58	PEHC	221---	2	A	2	C	PE-14	O	DS12.4
59	PETC	221---	2	A	2	D	PE-14	O	DS12.4
60	DCSS	2212--	2	I	2	A	SC-24	T	AI2.4
61	ECCD	2212--	2	I	2	B	AC-3	T	DS11.6
62	ECAT	221211	2	I	2	D	AU-6	T	DS5.5
63	IAKM	2213--	2	I	3	C	SC-12	T	DS5.8
64	CODB	321---	2	A	3	D	CP-9	O	DS11.5
65	CODP	321---	2	A	3	D	CP-2	O	DS4.2
66	COPS	321---	2	A	3	D	PE-11	O	DS12.4
67	DCAS	---111	3	C	1	A	SA-4	M	AI5.3
68	ECLP	---111	3	C	1	A	AC-6	T	DS5.4
69	ECRR	---111	3	I	1	C	AU-11	T	DS5.5
70	ECWM	---111	3	C	1	E	AC-8	T	DS5.7
71	PRNK	---111	3	C	1	A	PS-3	O	DS5.4
72	COBR	111---	3	A	1	A	CP-9	O	DS11.6
73	COSW	111---	3	A	1	A	CP-6	O	DS4.9
74	COTR	111---	3	A	1	A	CP-10	O	DS4.8
75	DCAR	111---	3	A	1	C	PL-2	M	DS5.2
76	DCBP	111---	3	I	1	C	IA-5	T	DS5.4
77	DCCT	111---	3	A	1	C	SA-11	M	AI6.2
78	DCDS	111---	3	I	1	C	SA-9	M	DS2.3
79	DCFA	111---	3	I	1	C	PL-2	M	PO2.1
80	DCHW	111---	3	A	1	A	CM-8	O	DS9.2
81	DCID	111---	3	I	1	A	CA-3	M	DS5.10
82	DCII	111---	3	I	1	C	CM-4	O	AI6.2
83	DCIT	111---	3	I	1	A	SA-9	M	DS1.3

#	ICG	Signature	Type	CIA	Span	Impact	Family	Class	Coverage
84	DCMC	111---	3	I	1	C	SC-18	T	DS5.9
85	DCNR	111---	3	I	1	C	AU-10	T	DS5.8
86	DCPD	111---	3	A	1	C	SA-6	M	AI5.3
87	DCPP	111---	3	A	1	C	CA-3	M	DS5.10
88	DCPR	111---	3	I	1	A	CM-9	O	DS9
89	DCSD	111---	3	A	1	A	PL-2	M	DS5.2
90	DCSL	111---	3	I	1	C	CM-5	O	DS11.3
91	DCSQ	111---	3	I	1	C	SA-11	M	AI2.8
92	DCSW	111---	3	A	1	A	CM-8	O	DS9.2
93	EBCR	111---	3	A	1	C	AC-4	T	DS5.10
94	EBVC	111---	3	A	1	C	SI-4	O	DS5.10
95	ECIM	111---	3	I	1	C	AC-4	T	DS5.10
96	ECPA	111---	3	I	1	A	AC-2	T	DS5.4
97	ECRG	111---	3	I	1	E	AU-7	T	DS5.5
98	ECSC	111---	3	A	1	A	CM-6	O	AI2.5
99	ECTP	111---	3	I	1	C	AU-9	T	DS11.6
100	ECVI	111---	3	A	1	C	SC-19	T	DS5.10
101	ECVP	111---	3	A	1	A	SI-3	O	DS5.9
102	ECWN	111---	3	A	1	A	AC-18	T	DS5.10
103	PEFI	111---	3	A	1	C	PE-13	O	DS12.4
104	PEMS	111---	3	A	1	A	PE-10	O	DS12.4
105	PESL	111---	3	I	1	C	AC-11	T	DS5.4
106	PETN	111---	3	A	1	E	AT-3	O	DS7.2
107	PEVR	111---	3	A	1	A	PE-9	O	DS12.4
108	PRRB	111---	3	A	1	A	PL-4	M	DS5.2
109	VIVM	111---	3	A	1	C	RA-5	M	DS5.2

3.2 CIA

This section explores the partition that 8500.2 provides via the listing of "Confidentiality," or "Integrity," or "Availability" at the right margin of each IAC appearance. This section concludes that the IACs follow the intent of the attachments, with a few exceptions and one apparent error.

It turns out that the 109 ICGs are distributed evenly, with only a slight emphasis on Availability and Confidentiality at the expense of Integrity, as shown in the next table.

Table 22 CIA Breakdown

CIA	ICGs	Percentage
Confidentiality	37	34%
Integrity	34	32%
Availability	38	34%
TOTAL	109	100%

Recall that the ICGs in Attachments A1, A2, and A3 are intended to focus on integrity or availability, that the ICGs in Attachments A4, A5, and A6 are intended to focus on confidentiality, and that the ICGs that focus on integrity or availability do not focus on confidentiality, and the converse. This is reflected in Pattern 2. All of the ICGs marked Availability are in Attachments A1, A2, and A3, and all of the ICGs marked Confidentiality are in Attachments A4, A5, and A6, as we would expect. The ICGs marked Integrity are in Attachments A1, A2, and A3, as we would expect, but five of them are also in Attachment A4, as we would not expect. These five ICGs are the same ones that do not conform to Pattern 2, described in the previous section as follows:

- Pattern 2:

  A given ICG that appears in Attachments A1 and/or A2 and/or A3 does not also appear in Attachments A4 and/or A5 and/or A6, and the converse. That is, an ICG appears in one set of attachments or the other: it does not appear in both sets.

The five, non-conforming ICGs are shown in the next table.

Table 23 CIA Non-Conforming ICGs

#	ICG	IA Control Name	Signature
35	ECTB	Audit Trail Backup	11-1--
60	DCSS	System State Changes	2212--
61	ECCD	Changes to Data	
62	ECAT	Audit Trail, Monitoring, Analysis and Reporting	221211 (equivalently 2212--)
63	IAKM	Key Management	2213--

All of the ICGs shown in the table above are marked "Integrity," suggesting that Attachments A1, A2, and A3 are their primary focus, with their appearances in Attachment A4 being of secondary importance.

There is one additional anomaly here. All of the IACs for a given ICG have the same CIA marking for each of their appearances, except for ICG #40 ECAR "Audit Record Content." ECAR's three appearances, IAC:213, IAC:256, and IAC:289, are in Attachments A4, A5, and A6, respectively, so ECAR conforms to Pattern 2. However, the first IAC is marked "Integrity" and the last two are marked "Confidentiality." Presumably, because all of the appearances are in Attachments A4, A5, and A6, the marking for IAC:213 is in error and should be "Confidentiality," like the other two.

The partition table, sorted on CIA, is shown below.

Table 24 Partition Table, Sorted on CIA

#	ICG	Signature	Type	CIA	Span	Impact	Family	Class	Coverage
31	DCPB	11----	1	A	1	A	SA-2	M	PO5.1
41	COEB	211---	2	A	2	B	PE-17	O	DS4.2
42	COED	211---	2	A	2	D	CP-4	O	DS4.5
43	COSP	211---	2	A	2	D	MA-6	O	DS1.3
44	VIIR	211---	2	A	2	B	IR-8	O	DS8
45	COAS	221---	2	A	2	B	CP-7	O	DS4.2
46	COEF	221---	2	A	2	D	CP-2	O	DS4.2
47	COMS	221---	2	A	2	D	MA-6	O	DS1.3
55	PEEL	221---	2	A	2	D	PE-12	O	DS12.4
56	PEFD	221---	2	A	2	A	PE-13	O	DS12.4
57	PEFS	221---	2	A	2	B	PE-13	O	DS12.4
58	PEHC	221---	2	A	2	C	PE-14	O	DS12.4
59	PETC	221---	2	A	2	D	PE-14	O	DS12.4
64	CODB	321---	2	A	3	D	CP-9	O	DS11.5
65	CODP	321---	2	A	3	D	CP-2	O	DS4.2
66	COPS	321---	2	A	3	D	PE-11	O	DS12.4
72	COBR	111---	3	A	1	A	CP-9	O	DS11.6
73	COSW	111---	3	A	1	A	CP-6	O	DS4.9
74	COTR	111---	3	A	1	A	CP-10	O	DS4.8
75	DCAR	111---	3	A	1	C	PL-2	M	DS5.2
77	DCCT	111---	3	A	1	C	SA-11	M	AI6.2
80	DCHW	111---	3	A	1	A	CM-8	O	DS9.2
86	DCPD	111---	3	A	1	C	SA-6	M	AI5.3
87	DCPP	111---	3	A	1	C	CA-3	M	DS5.10
89	DCSD	111---	3	A	1	A	PL-2	M	DS5.2
92	DCSW	111---	3	A	1	A	CM-8	O	DS9.2
93	EBCR	111---	3	A	1	C	AC-4	T	DS5.10
94	EBVC	111---	3	A	1	C	SI-4	O	DS5.10
98	ECSC	111---	3	A	1	A	CM-6	O	AI2.5
100	ECVI	111---	3	A	1	C	SC-19	T	DS5.10

#	ICG	Signature	Type	CIA	Span	Impact	Family	Class	Coverage
101	ECVP	111---	3	A	1	A	SI-3	O	DS5.9
102	ECWN	111---	3	A	1	A	AC-18	T	DS5.10
103	PEFI	111---	3	A	1	C	PE-13	O	DS12.4
104	PEMS	111---	3	A	1	A	PE-10	O	DS12.4
106	PETN	111---	3	A	1	E	AT-3	O	DS7.2
107	PEVR	111---	3	A	1	A	PE-9	O	DS12.4
108	PRRB	111---	3	A	1	A	PL-4	M	DS5.2
109	VIVM	111---	3	A	1	C	RA-5	M	DS5.2
1	ECNK	---1+21-	0	C	2	C	SC-9	T	DS5.11
2	ECCR	---2+31-	0	C	2	Z	SC-28	T	DS11.6
3	ECCT	---21-	0	C	2	B	SC-9	T	DS5.11
4	ECLO	---21-	0	C	2	C	AC-7	T	DS5.4
5	IAIA	---21-	0	C	2	A	IA-5	T	DS5.4
6	PECF	---21-	0	C	2	A	PE-2	O	DS12.3
7	PECS	---21-	0	C	2	A	MP-6	O	DS5.11
8	PEPF	---21-	0	C	2	A	PE-3	O	DS12.3
9	PRAS	---21-	0	C	2	A	PS-3	O	DS5.4
10	EBPW	----11	1	C	1	A	SC-7	T	DS5.10
11	ECCM	---1--	1	C	1	A	SC-12	T	DS5.8
12	ECLC	---1--	1	C	1	E	AU-3	T	DS5.5
13	PEDD	---1--	1	C	1	A	MP-6	O	DS11.4
14	EBRP	---11-	1	C	1	A	AC-17	T	DS5.10
15	EBRU	---11-	1	C	1	A	AC-17	T	DS5.10
16	ECAD	---11-	1	C	1	C	AC-3	T	DS5.3
17	ECAN	---11-	1	C	1	A	AC-3	T	DS5.4
18	ECIC	---11-	1	C	1	C	AC-4	T	DS5.10
19	ECML	---11-	1	C	1	A	MP-3	O	DS11.6
20	ECRC	---11-	1	C	1	C	SC-4	T	DS11.6
21	ECTC	---11-	1	C	1	A	PE-19	O	DS5.5
22	IAAC	---11-	1	C	1	A	AC-2	T	DS5.4
23	IAGA	---11-	1	C	1	C	IA-2	T	DS5.4
24	PEDI	---11-	1	C	1	A	PE-5	O	DS11.6
25	PEPS	---11-	1	C	1	E	PE-3	O	DS12.2
26	PESP	---11-	1	C	1	C	PL-4	M	DS11.6
27	PESS	---11-	1	C	1	A	MP-4	O	DS11.2
28	PEVC	---11-	1	C	1	A	PE-7+8	O	DS12.3
36	ECMT	---211	2	C	2	D	CA-7	M	ME2.4
37	PRMP	---211	2	C	2	A	MA-5	O	DS1.3
38	DCSR	---321	2	C	3	A	SA-14	M	DS5.2
39	EBBD	---321	2	C	3	Z	SC-7	T	DS5.10
67	DCAS	---111	3	C	1	A	SA-4	M	AI5.3
68	ECLP	---111	3	C	1	A	AC-6	T	DS5.4
70	ECWM	---111	3	C	1	E	AC-8	T	DS5.7
71	PRNK	---111	3	C	1	A	PS-3	O	DS5.4

#	ICG	Signature	Type	CIA	Span	Impact	Family	Class	Coverage
29	PRTN	---11-	1	I	1	A	AT-3	O	DS7.2
30	DCPA	11----	1	I	1	E	SC-2	T	DS11.6
32	DCSP	11----	1	I	1	C	SC-3	T	DS5.7
33	ECDC	11----	1	I	1	C	CP-10	O	DS11.6
34	ECID	11----	1	I	1	C	SI-4	O	DS5.9
35	ECTB	11-1--	1	I	1	C	AU-9	T	DS11.5
48	DCCB	221---	2	I	2	D	CM-3	O	DS9
49	DCCS	221---	2	I	2	A	CM-6	O	DS9.1
50	ECND	221---	2	I	2	D	SC-7	T	DS5.10
51	ECPC	221---	2	I	2	C	AC-2	T	DS5.4
52	ECSD	221---	2	I	2	B	CM-5	O	DS11.3
53	ECTM	221---	2	I	2	C	SC-8	T	DS5.11
54	IATS	221---	2	I	2	C	IA-5	T	DS5.8
60	DCSS	2212--	2	I	2	A	SC-24	T	AI2.4
61	ECCD	2212--	2	I	2	B	AC-3	T	DS11.6
62	ECAT	221211	2	I	2	D	AU-6	T	DS5.5
63	IAKM	2213--	2	I	3	C	SC-12	T	DS5.8
69	ECRR	---111	3	I	1	C	AU-11	T	DS5.5
76	DCBP	111---	3	I	1	C	IA-5	T	DS5.4
78	DCDS	111---	3	I	1	C	SA-9	M	DS2.3
79	DCFA	111---	3	I	1	C	PL-2	M	PO2.1
81	DCID	111---	3	I	1	A	CA-3	M	DS5.10
82	DCII	111---	3	I	1	C	CM-4	O	AI6.2
83	DCIT	111---	3	I	1	A	SA-9	M	DS1.3
84	DCMC	111---	3	I	1	C	SC-18	T	DS5.9
85	DCNR	111---	3	I	1	C	AU-10	T	DS5.8
88	DCPR	111---	3	I	1	A	CM-9	O	DS9
90	DCSL	111---	3	I	1	C	CM-5	O	DS11.3
91	DCSQ	111---	3	I	1	C	SA-11	M	AI2.8
95	ECIM	111---	3	I	1	C	AC-4	T	DS5.10
96	ECPA	111---	3	I	1	A	AC-2	T	DS5.4
97	ECRG	111---	3	I	1	E	AU-7	T	DS5.5
99	ECTP	111---	3	I	1	C	AU-9	T	DS11.6
105	PESL	111---	3	I	1	C	AC-11	T	DS5.4
40	ECAR	---321	2	ICC	3	Z	AU-3	T	DS5.5

3.3 Span

This section explores the concept of "span." This concept identifies the ICGs for which robustness is important.

As was explained in the Introduction above, the integer after the dash in an IACN indicates the "robustness" or rigor of the IAC. The minimum robustness is 1, the maximum is 3, and ICGs follow the Robustness Rule, as presented in the Introduction above and, for ease of reference, is copied here:

> All ICGs have an IAC with robustness 1 but only ICGs that have an IAC with robustness 2 have an IAC with robustness 3.

We introduce the term "span" to indicate the robustness range for each ICG.

We would expect that the ICGs would be evenly distributed across the Spans—that 1/3 (about 36) of the ICGs would be in each span category. This is almost the case for Span 2 but the remainder of the ICGs are weighted toward Span 1 with only a handful ICGs in Span 3, as shown in the next table.

Table 25 Span Breakdown

Span	ICGs	Percentage
1	69	64%
2	33	30%
3	7	6%
TOTAL	109	100%

Of interest are the seven Span 3 ICGs, shown in the next table.

Table 26 Span 3 ICGs

#	ICG	IA Control Name	Signature
38	DCSR	Specified Robustness	---321
39	EBBD	Boundary Defense	
40	ECAR	Audit Record Content	
63	IAKM	Key Management	2213--
64	CODB	Data Backup Procedures	321---
65	CODP	Disaster and Recovery Planning	
66	COPS	Power Supply	

DCSR needs to have Span 3, by the definition of this ICG, but there is no obvious, corresponding need for the other six ICGs. The fact that the DoD chose only six ICGs, and not the expected 36, to have Span 3 highlights the importance of these particular ICGs.

Note that type and span are related because both depend upon robustness. All Type 0 ICGs must be Span 2. All Type 1 and Type 3 ICGs must be Span 1. And all Type 2 ICGS must be either Span 2 or Span 3, as shown in the next table.

Table 27 Span & Type

Span	Type			
	0	1	2	3
1		X		X
2	X		X	
3			X	

The partition table, sorted on Span, is shown below.

Table 28 Partition Table, Sorted on Span

#	ICG	Signature	Type	CIA	Span	Impact	Family	Class	Coverage
10	EBPW	----11	1	C	1	A	SC-7	T	DS5.10
11	ECCM	---1--	1	C	1	A	SC-12	T	DS5.8
12	ECLC	---1--	1	C	1	E	AU-3	T	DS5.5
13	PEDD	---1--	1	C	1	A	MP-6	O	DS11.4
14	EBRP	---11-	1	C	1	A	AC-17	T	DS5.10
15	EBRU	---11-	1	C	1	A	AC-17	T	DS5.10
16	ECAD	---11-	1	C	1	C	AC-3	T	DS5.3
17	ECAN	---11-	1	C	1	A	AC-3	T	DS5.4
18	ECIC	---11-	1	C	1	C	AC-4	T	DS5.10
19	ECML	---11-	1	C	1	A	MP-3	O	DS11.6
20	ECRC	---11-	1	C	1	C	SC-4	T	DS11.6
21	ECTC	---11-	1	C	1	A	PE-19	O	DS5.5
22	IAAC	---11-	1	C	1	A	AC-2	T	DS5.4
23	IAGA	---11-	1	C	1	C	IA-2	T	DS5.4
24	PEDI	---11-	1	C	1	A	PE-5	O	DS11.6
25	PEPS	---11-	1	C	1	E	PE-3	O	DS12.2
26	PESP	---11-	1	C	1	C	PL-4	M	DS11.6
27	PESS	---11-	1	C	1	A	MP-4	O	DS11.2
28	PEVC	---11-	1	C	1	A	PE-7+8	O	DS12.3
29	PRTN	---11-	1	I	1	A	AT-3	O	DS7.2
30	DCPA	11----	1	I	1	E	SC-2	T	DS11.6
31	DCPB	11----	1	A	1	A	SA-2	M	PO5.1
32	DCSP	11----	1	I	1	C	SC-3	T	DS5.7
33	ECDC	11----	1	I	1	C	CP-10	O	DS11.6
34	ECID	11----	1	I	1	C	SI-4	O	DS5.9
35	ECTB	11-1--	1	I	1	C	AU-9	T	DS11.5
67	DCAS	---111	3	C	1	A	SA-4	M	AI5.3
68	ECLP	---111	3	C	1	A	AC-6	T	DS5.4
69	ECRR	---111	3	I	1	C	AU-11	T	DS5.5
70	ECWM	---111	3	C	1	E	AC-8	T	DS5.7
71	PRNK	---111	3	C	1	A	PS-3	O	DS5.4

#	ICG	Signature	Type	CIA	Span	Impact	Family	Class	Coverage
72	COBR	111---	3	A	1	A	CP-9	O	DS11.6
73	COSW	111---	3	A	1	A	CP-6	O	DS4.9
74	COTR	111---	3	A	1	A	CP-10	O	DS4.8
75	DCAR	111---	3	A	1	C	PL-2	M	DS5.2
76	DCBP	111---	3	I	1	C	IA-5	T	DS5.4
77	DCCT	111---	3	A	1	C	SA-11	M	AI6.2
78	DCDS	111---	3	I	1	C	SA-9	M	DS2.3
79	DCFA	111---	3	I	1	C	PL-2	M	PO2.1
80	DCHW	111---	3	A	1	A	CM-8	O	DS9.2
81	DCID	111---	3	I	1	A	CA-3	M	DS5.10
82	DCII	111---	3	I	1	C	CM-4	O	AI6.2
83	DCIT	111---	3	I	1	A	SA-9	M	DS1.3
84	DCMC	111---	3	I	1	C	SC-18	T	DS5.9
85	DCNR	111---	3	I	1	C	AU-10	T	DS5.8
86	DCPD	111---	3	A	1	C	SA-6	M	AI5.3
87	DCPP	111---	3	A	1	C	CA-3	M	DS5.10
88	DCPR	111---	3	I	1	A	CM-9	O	DS9
89	DCSD	111---	3	A	1	A	PL-2	M	DS5.2
90	DCSL	111---	3	I	1	C	CM-5	O	DS11.3
91	DCSQ	111---	3	I	1	C	SA-11	M	AI2.8
92	DCSW	111---	3	A	1	A	CM-8	O	DS9.2
93	EBCR	111---	3	A	1	C	AC-4	T	DS5.10
94	EBVC	111---	3	A	1	C	SI-4	O	DS5.10
95	ECIM	111---	3	I	1	C	AC-4	T	DS5.10
96	ECPA	111---	3	I	1	A	AC-2	T	DS5.4
97	ECRG	111---	3	I	1	E	AU-7	T	DS5.5
98	ECSC	111---	3	A	1	A	CM-6	O	AI2.5
99	ECTP	111---	3	I	1	C	AU-9	T	DS11.6
100	ECVI	111---	3	A	1	C	SC-19	T	DS5.10
101	ECVP	111---	3	A	1	A	SI-3	O	DS5.9
102	ECWN	111---	3	A	1	A	AC-18	T	DS5.10
103	PEFI	111---	3	A	1	C	PE-13	O	DS12.4
104	PEMS	111---	3	A	1	A	PE-10	O	DS12.4
105	PESL	111---	3	I	1	C	AC-11	T	DS5.4
106	PETN	111---	3	A	1	E	AT-3	O	DS7.2
107	PEVR	111---	3	A	1	A	PE-9	O	DS12.4
108	PRRB	111---	3	A	1	A	PL-4	M	DS5.2
109	VIVM	111---	3	A	1	C	RA-5	M	DS5.2
1	ECNK	---1+21-	0	C	2	C	SC-9	T	DS5.11
2	ECCR	---2+31-	0	C	2[21]	Z	SC-28	T	DS11.6
3	ECCT	---21-	0	C	2	B	SC-9	T	DS5.11

[21] ECNK's span is 2, not 3, because ECNK-3 should properly be combined with ECNK-2, which would change the signature from ---2+31 to ---21- (see "Type" section).

#	ICG	Signature	Type	CIA	Span	Impact	Family	Class	Coverage
4	ECLO	---21-	0	C	2	C	AC-7	T	DS5.4
5	IAIA	---21-	0	C	2	A	IA-5	T	DS5.4
6	PECF	---21-	0	C	2	A	PE-2	O	DS12.3
7	PECS	---21-	0	C	2	A	MP-6	O	DS5.11
8	PEPF	---21-	0	C	2	A	PE-3	O	DS12.3
9	PRAS	---21-	0	C	2	A	PS-3	O	DS5.4
36	ECMT	---211	2	C	2	D	CA-7	M	ME2.4
37	PRMP	---211	2	C	2	A	MA-5	O	DS1.3
41	COEB	211---	2	A	2	B	PE-17	O	DS4.2
42	COED	211---	2	A	2	D	CP-4	O	DS4.5
43	COSP	211---	2	A	2	D	MA-6	O	DS1.3
44	VIIR	211---	2	A	2	B	IR-8	O	DS8
45	COAS	221---	2	A	2	B	CP-7	O	DS4.2
46	COEF	221---	2	A	2	D	CP-2	O	DS4.2
47	COMS	221---	2	A	2	D	MA-6	O	DS1.3
48	DCCB	221---	2	I	2	D	CM-3	O	DS9
49	DCCS	221---	2	I	2	A	CM-6	O	DS9.1
50	ECND	221---	2	I	2	D	SC-7	T	DS5.10
51	ECPC	221---	2	I	2	C	AC-2	T	DS5.4
52	ECSD	221---	2	I	2	B	CM-5	O	DS11.3
53	ECTM	221---	2	I	2	C	SC-8	T	DS5.11
54	IATS	221---	2	I	2	C	IA-5	T	DS5.8
55	PEEL	221---	2	A	2	D	PE-12	O	DS12.4
56	PEFD	221---	2	A	2	A	PE-13	O	DS12.4
57	PEFS	221---	2	A	2	B	PE-13	O	DS12.4
58	PEHC	221---	2	A	2	C	PE-14	O	DS12.4
59	PETC	221---	2	A	2	D	PE-14	O	DS12.4
60	DCSS	2212--	2	I	2	A	SC-24	T	AI2.4
61	ECCD	2212--	2	I	2	B	AC-3	T	DS11.6
62	ECAT	221211	2	I	2	D	AU-6	T	DS5.5
38	DCSR	---321	2	C	3	A	SA-14	M	DS5.2
39	EBBD	---321	2	C	3	Z	SC-7	T	DS5.10
40	ECAR	---321	2	ICC	3	Z	AU-3	T	DS5.5
63	IAKM	2213--	2	I	3	C	SC-12	T	DS5.8
64	CODB	321---	2	A	3	D	CP-9	O	DS11.5
65	CODP	321---	2	A	3	D	CP-2	O	DS4.2
66	COPS	321---	2	A	3	D	PE-11	O	DS12.4

3.4 Impact

This section explores the concept of "impact" and organizes the ICGs into six impact "priorities."

The following passage from DIACAP explains the origin and meaning of "impact" as it pertains to ICGs (and IACs):

> Impact codes are assigned by the TAG [Technical Advisory Group] to IA controls at the time of authoring and are maintained through the DIACAP CCM [Configuration and Control Management]. They indicate the TAG's assessment of the consequences of a failed IA control. Impact codes are expressed as high, medium, and low, with high indicating the greatest impact. In conjunction with the severity category,[22] the impact code indicates the urgency with which corrective action should be taken. Within a severity category, non-compliant IA controls should be prioritized for correction or remediation according to their impact codes. (DIACAP [4], Paragraph 6.3.3.1.3, page 17)[23]

Given the preceding description, "impact" could also be called "relative urgency of compliance."

The IACs in an ICG can have different impacts, as will be shown below.

Impact is different than robustness. Robustness is defined as a "characterization of the strength of a security function, mechanism, service or solution, and the assurance (or confidence) that it is implemented and functioning correctly" (8500.2, page 23). Robustness does not include the priority relative to other ICGs with which non-compliance should be addressed.

We can construct an "impact" signature that parallels the signature for robustness, as developed in the section above on types, by replacing each integer in the robustness signature with the corresponding impact. This gives us an impact signature such as ---LMH for EBBD.

There are some impact signatures that have only one level of impact, such as ---LL-, and there are other signatures that have two levels of impact, such as LMM---, and finally there are signatures that have all three levels, such as ---LMH. The signatures fall into six partition

---

[22] The "severity category" (i.e., "CAT I," "CAT II," "CAT III") of a "system weakness or shortcoming," as DIACAP defines it, indicates the "risk level" and the "urgency with which the corrective action must be completed." Unlike impact codes which are assigned by the TAG [the DIACAP Technical Advisory Group] and are irrespective of a given system, a severity code is assigned by a "CA [Certifying Authority] or a designated representative" "after considering all possible mitigation measures that have been implemented within system design and architecture limitations for the DoD IS [information system] in question" (DIACAP [4], Paragraph 6.3.3.1.4, page 17).

[23] The Impact codes are available from DoD's Knowledge Service [5].

subsets that this report calls impact "priorities." The impact priorities, their descriptions, an example, and the number and percentage of ICGs of each priority are shown in the next table.

Table 29 Impact Priorities Breakdown

Impact Priority	Description	Example	Number of ICGs	% of ICGs
A	All impact codes are high	HHH---	43	39%
B	All impact codes are medium or high	---HM-	7	6%
C	All impact codes are medium	MMM---	37	34%
D	All impact codes are medium or low	LMM---	13	12%
E	All impact codes are low	---LL-	6	6%
Z	All three impact codes appear	---LMH	3	3%
TOTAL			109	100%

The set of impact priorities constitute a partially ordered set. For example, the ICGs of Impact Priority A always have a higher impact than ICGs of Impact Priorities C, D, and E but only sometimes higher than Impact Priorities B and Z. Similarly, the ICGs of Impact Priority E always have a lower impact than ICGs of Impact Priorities A, B, and C but only sometimes lower than Impact Priorities D and Z, as shown in the following figure.

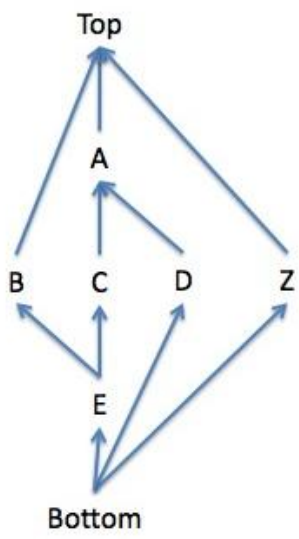

Figure 1 Impact Poset

If the 109 ICGs were evenly distributed across the six priorities, we would see approximately 18 ICGs in each priority. Priorities A and C each has more than 1/3 of the ICGs which is twice what we expect. Priority D has the number we expect and Priorities B, E, and Z have far fewer

ICGs than we expect. This represents an emphasis on Priority A and a significant de-emphasis of Priority E. This suggests an unwillingness to label a control as low priority. Unfortunately, this unwillingness weakens the impact concept. (In the extreme case, all ICGs would be Impact Priority A, which would eliminate the value of priority.)

The six ICGs with Impact Priority E are shown in the next table.

Table 30 Impact Priority E ICGs

#	ICG	IA Control Name
12	ECLC	Audit of Security Label Changes
25	PEPS	Physical Security Testing
30	DCPA	Partitioning the Application
70	ECWM	Warning Message
97	ECRG	Audit Reduction and Report Generation
106	PETN	Environmental Training

The impact for these ICGs seems to be appropriately assigned: they all seem the sort the compliance for which can always wait.

The three ICGs with Impact Priority Z are shown in the next table.

Table 31 Impact Priority Z ICGs

#	ICG	IA Control Name	Signature	Impact Signature
2	ECCR	Encryption for Confidentiality (Data at Rest)	---2+31-	---M+HL-
39	EBBD	Boundary Defense	---321	---LMH
40	ECAR	Audit Record Content		

All three of these ICGs have right signatures (i.e., they are found in Attachments A4, A5, and A6[24] only) and they all seem the sort the compliance for which is increasingly important as we move from Public to Sensitive to Classified. ECCR's impact signature, ---M+HL-, is as we expect, but the impact signature for both EBBD and ECAR is ---LMH, not ---HML, suggesting that the jump from no boundary defense and auditing to some is of greater urgency than the jump from some to more.

The partition table, sorted on Impact, is shown below.

Table 32 Partition Table, Sorted on Impact

#	ICG	Signature	Type	CIA	Span	Impact	Family	Class	Coverage
5	IAIA	---21-	0	C	2	A	IA-5	T	DS5.4
6	PECF	---21-	0	C	2	A	PE-2	O	DS12.3
7	PECS	---21-	0	C	2	A	MP-6	O	DS5.11
8	PEPF	---21-	0	C	2	A	PE-3	O	DS12.3

[24] ECCR and EBBD are both marked "Confidentiality," as we would expect, but ECAR is marked "Integrity."

#	ICG	Signature	Type	CIA	Span	Impact	Family	Class	Coverage
9	PRAS	---21-	0	C	2	A	PS-3	O	DS5.4
10	EBPW	----11	1	C	1	A	SC-7	T	DS5.10
11	ECCM	---1--	1	C	1	A	SC-12	T	DS5.8
13	PEDD	---1--	1	C	1	A	MP-6	O	DS11.4
14	EBRP	---11-	1	C	1	A	AC-17	T	DS5.10
15	EBRU	---11-	1	C	1	A	AC-17	T	DS5.10
17	ECAN	---11-	1	C	1	A	AC-3	T	DS5.4
19	ECML	---11-	1	C	1	A	MP-3	O	DS11.6
21	ECTC	---11-	1	C	1	A	PE-19	O	DS5.5
22	IAAC	---11-	1	C	1	A	AC-2	T	DS5.4
24	PEDI	---11-	1	C	1	A	PE-5	O	DS11.6
27	PESS	---11-	1	C	1	A	MP-4	O	DS11.2
28	PEVC	---11-	1	C	1	A	PE-7+8	O	DS12.3
29	PRTN	---11-	1	I	1	A	AT-3	O	DS7.2
31	DCPB	11----	1	A	1	A	SA-2	M	PO5.1
37	PRMP	---211	2	C	2	A	MA-5	O	DS1.3
38	DCSR	---321	2	C	3	A	SA-14	M	DS5.2
49	DCCS	221---	2	I	2	A	CM-6	O	DS9.1
56	PEFD	221---	2	A	2	A	PE-13	O	DS12.4
60	DCSS	2212--	2	I	2	A	SC-24	T	AI2.4
67	DCAS	---111	3	C	1	A	SA-4	M	AI5.3
68	ECLP	---111	3	C	1	A	AC-6	T	DS5.4
71	PRNK	---111	3	C	1	A	PS-3	O	DS5.4
72	COBR	111---	3	A	1	A	CP-9	O	DS11.6
73	COSW	111---	3	A	1	A	CP-6	O	DS4.9
74	COTR	111---	3	A	1	A	CP-10	O	DS4.8
80	DCHW	111---	3	A	1	A	CM-8	O	DS9.2
81	DCID	111---	3	I	1	A	CA-3	M	DS5.10
83	DCIT	111---	3	I	1	A	SA-9	M	DS1.3
88	DCPR	111---	3	I	1	A	CM-9	O	DS9
89	DCSD	111---	3	A	1	A	PL-2	M	DS5.2
92	DCSW	111---	3	A	1	A	CM-8	O	DS9.2
96	ECPA	111---	3	I	1	A	AC-2	T	DS5.4
98	ECSC	111---	3	A	1	A	CM-6	O	AI2.5
101	ECVP	111---	3	A	1	A	SI-3	O	DS5.9
102	ECWN	111---	3	A	1	A	AC-18	T	DS5.10
104	PEMS	111---	3	A	1	A	PE-10	O	DS12.4
107	PEVR	111---	3	A	1	A	PE-9	O	DS12.4
108	PRRB	111---	3	A	1	A	PL-4	M	DS5.2
3	ECCT	---21-	0	C	2	B	SC-9	T	DS5.11
41	COEB	211---	2	A	2	B	PE-17	O	DS4.2
44	VIIR	211---	2	A	2	B	IR-8	O	DS8
45	COAS	221---	2	A	2	B	CP-7	O	DS4.2
52	ECSD	221---	2	I	2	B	CM-5	O	DS11.3

#	ICG	Signature	Type	CIA	Span	Impact	Family	Class	Coverage
57	PEFS	221---	2	A	2	B	PE-13	O	DS12.4
61	ECCD	2212--	2	I	2	B	AC-3	T	DS11.6
1	ECNK	---1+21-	0	C	2	C	SC-9	T	DS5.11
4	ECLO	---21-	0	C	2	C	AC-7	T	DS5.4
16	ECAD	---11-	1	C	1	C	AC-3	T	DS5.3
18	ECIC	---11-	1	C	1	C	AC-4	T	DS5.10
20	ECRC	---11-	1	C	1	C	SC-4	T	DS11.6
23	IAGA	---11-	1	C	1	C	IA-2	T	DS5.4
26	PESP	---11-	1	C	1	C	PL-4	M	DS11.6
32	DCSP	11----	1	I	1	C	SC-3	T	DS5.7
33	ECDC	11----	1	I	1	C	CP-10	O	DS11.6
34	ECID	11----	1	I	1	C	SI-4	O	DS5.9
35	ECTB	11-1--	1	I	1	C	AU-9	T	DS11.5
51	ECPC	221---	2	I	2	C	AC-2	T	DS5.4
53	ECTM	221---	2	I	2	C	SC-8	T	DS5.11
54	IATS	221---	2	I	2	C	IA-5	T	DS5.8
58	PEHC	221---	2	A	2	C	PE-14	O	DS12.4
63	IAKM	2213--	2	I	3	C	SC-12	T	DS5.8
69	ECRR	---111	3	I	1	C	AU-11	T	DS5.5
75	DCAR	111---	3	A	1	C	PL-2	M	DS5.2
76	DCBP	111---	3	I	1	C	IA-5	T	DS5.4
77	DCCT	111---	3	A	1	C	SA-11	M	AI6.2
78	DCDS	111---	3	I	1	C	SA-9	M	DS2.3
79	DCFA	111---	3	I	1	C	PL-2	M	PO2.1
82	DCII	111---	3	I	1	C	CM-4	O	AI6.2
84	DCMC	111---	3	I	1	C	SC-18	T	DS5.9
85	DCNR	111---	3	I	1	C	AU-10	T	DS5.8
86	DCPD	111---	3	A	1	C	SA-6	M	AI5.3
87	DCPP	111---	3	A	1	C	CA-3	M	DS5.10
90	DCSL	111---	3	I	1	C	CM-5	O	DS11.3
91	DCSQ	111---	3	I	1	C	SA-11	M	AI2.8
93	EBCR	111---	3	A	1	C	AC-4	T	DS5.10
94	EBVC	111---	3	A	1	C	SI-4	O	DS5.10
95	ECIM	111---	3	I	1	C	AC-4	T	DS5.10
99	ECTP	111---	3	I	1	C	AU-9	T	DS11.6
100	ECVI	111---	3	A	1	C	SC-19	T	DS5.10
103	PEFI	111---	3	A	1	C	PE-13	O	DS12.4
105	PESL	111---	3	I	1	C	AC-11	T	DS5.4
109	VIVM	111---	3	A	1	C	RA-5	M	DS5.2
36	ECMT	---211	2	C	2	D	CA-7	M	ME2.4
42	COED	211---	2	A	2	D	CP-4	O	DS4.5
43	COSP	211---	2	A	2	D	MA-6	O	DS1.3
46	COEF	221---	2	A	2	D	CP-2	O	DS4.2
47	COMS	221---	2	A	2	D	MA-6	O	DS1.3

#	ICG	Signature	Type	CIA	Span	Impact	Family	Class	Coverage
48	DCCB	221---	2	I	2	D	CM-3	O	DS9
50	ECND	221---	2	I	2	D	SC-7	T	DS5.10
55	PEEL	221---	2	A	2	D	PE-12	O	DS12.4
59	PETC	221---	2	A	2	D	PE-14	O	DS12.4
62	ECAT	221211	2	I	2	D	AU-6	T	DS5.5
64	CODB	321---	2	A	3	D	CP-9	O	DS11.5
65	CODP	321---	2	A	3	D	CP-2	O	DS4.2
66	COPS	321---	2	A	3	D	PE-11	O	DS12.4
12	ECLC	---1--	1	C	1	E	AU-3	T	DS5.5
25	PEPS	---11-	1	C	1	E	PE-3	O	DS12.2
30	DCPA	11----	1	I	1	E	SC-2	T	DS11.6
70	ECWM	---111	3	C	1	E	AC-8	T	DS5.7
97	ECRG	111---	3	I	1	E	AU-7	T	DS5.5
106	PETN	111---	3	A	1	E	AT-3	O	DS7.2
2	ECCR	---2+31-	0	C	2	Z	SC-28	T	DS11.6
39	EBBD	---321	2	C	3	Z	SC-7	T	DS5.10
40	ECAR	---321	2	ICC	3	Z	AU-3	T	DS5.5

3.5 Family

This section explores a partition based on another set of controls, namely the controls in NIST 800-53 [10] (hereafter "800-53"). This exercise provides perspective on the ICGs.

The 800-53 controls are grouped in to 18 "families." At least one ICG maps to each family but almost half of the ICGs map to the following three families:

- Access Control (AC),
- Physical & Environmental Protection (PE), and
- System & Communication Protection (SC)

This suggests an emphasis by the ICGs on these three areas.

NIST, like the DoD, is a federal agency. While DoD provides controls for the DoD, NIST provides controls for the other federal agencies, except for the intelligence agencies. The close organizational ties between NIST and DoD suggest that the controls generated by NIST will correlate well with those from DoD.

800-53, like 8500.2, categorizes systems. 800-53's categorization is based on the FIPS 199 [6] approach of using the potential impact of a loss of confidentiality, integrity, and availability, where "impact" can be low, moderate, or high.[25] There are thus 27 categories of systems. However, NIST reduces the 27 categories in FIPS 200 [7] to three: low, moderate, and high, depending on the highest potential impact of a loss of confidentiality, integrity, and availability.[26] With that introduction, we can present 800-53's structure.

800-53 has a three-tiered structure with

1. 18 "families" which consist of…

---

[25] "Impact" as it is used in 800-53 is independent of "impact" as it is used in DIACAP [4] (and as explained in the previous section of this report).

[26] A system's category can be represented by an ordered triple. For example, the category <Low, Moderate, High> can represent systems with a low confidentiality impact, a moderate integrity impact, and a high availability impact. 800-53 uses the FIPS 200 concept of a "high water mark:" the highest impact in a triple determines the system category. The high water mark concept reduces the categories down to three, as noted in the text. Unfortunately the population of the systems in the three categories is not evenly distributed but is weighted toward high-impact. Of the 27 system types, there is only one triple—which constitute 4% of the triples—of low-impact systems, namely <Low, Low, Low>. There are seven moderate-impact systems, which constitute 25% of the triples, namely <Moderate, Low, Low>, <Low, Moderate, Low>, <Low, Low, Moderate>, <Moderate, Moderate, Low>, <Moderate, Low, Moderate>, <Low, Moderate, Moderate>, <Moderate, Moderate, Moderate>. The remaining 19 triples, which constitute 70% of the triples, are all high-impact systems.

2. 198 controls (not including (a) the 20 controls that are marked "Not Selected" in the listing in 800-53 and (b) the 6 controls that are marked "Withdrawn" in the listing in 800-53[27]), each of which consists of…
3. the following
    a. a paragraph describing the "Control,"
    b. a paragraph providing "Supplemental Guidance," and
    c. a number of paragraphs describing "Control Enhancements," where the Control Enhancements for low systems are a subset (not necessarily proper) of the Control Enhancements for moderate systems, which, in turn, are a subset (again, not necessarily proper) of the Control Enhancements for high systems (and some Control Enhancements are not in any of these sets but are included for general consideration).

800-53's structure is summarized in the next table.

Table 33 NIST 800-53 Structure

Level	Name	Items
1	Family	18
2	Control	198
3	Control Enhancement	Approximately 420

Three of 800-53's family names and 8500.2's subject areas share meaning:

1. The 800-53 family name "Identification and Authentication," matches the 8500.2 subject area with the same name.
2. The 800-53 family name "Contingency Planning" has the same general meaning as the 8500.2 subject area "Continuity."
3. The 800-53 family name "Incident Response" is a subset of the 8500.2 subject area "Vulnerability and Incident Response."

The next table shows the number of ICGs that map to each family of 800-53. Although 800-53 provides mapping from 800-53 to ISO/IEC 27001[28] it does not provide a mapping to 8500.2, so the mapping shown in the next table has been generated for this report.[29]

---

[27] In addition to the items selected for low, medium, and high systems, 800-53 includes "Not Selected" and "Withdrawn" items, as noted here. The "Not Selected" items are provided "for use by organizations if needed" (800-53, page D-1) but no suggestions are provided on how to determine relevance for a given system. Meanwhile, 800-53 does not tell us the meaning of "Withdrawn" so we presume that it means that these controls were in some previous version and are anticipated not to appear in some future edition but are present in the current edition in order to provide continuity.

[28] See Appendix H of 800-53.

[29] There are only several ICGs for which the mapping to the 800-53 controls is not straightforward, each described below in this footnote.

The mapping is shown at the family level in the next table because we are interested in partitioning based on the families. However, the partition table also shows the mapping at the control level. This finer-grained mapping provides better support for this subjective process.

Table 34 Mapping ICGs to NIST 800-53 Families[30]

Identifier	Family	Class[31]	Controls[32]	Matching ICGs from 8500.2
AC	Access Control	Technical	19	16
AT	Awareness and Training	Operational	5	2
AU	Audit and Accountability	Technical	14	8
CA[33]	Security Assessment and Authorization	Management	6	3
CM	Configuration Management	Operational	9	9
CP	Contingency Planning	Operational	9	9
IA	Identification and Authentication	Technical	8	4
IR	Incident Response	Operational	8	1
MA	Maintenance	Operational	6	3

---

(1) ECAD "Affiliation Display" requires that contractors and foreign nationals have e-mail addresses that indicate their affiliation. 800-53 does not mention e-mail addresses. However, AC-3 "Access Enforcement" calls for access control policies that could include groups such as contractors and foreign nationals.

(2) ECLC "Audit of Security Label Changes" maps to AU-3 "Content of Audit Records" because AU-3 provides a minimum list of items to audit, to which the auditing of security label changes could be added. (AC-16 "Security Attributes" describes security labels but does not address the auditing of those labels.)

(3) ECND "Network Device Controls" describes an "effective network device program," i.e., how to provide effective network security. SC-7 "Boundary Protection," on the other hand, describes the goals of effective network security. In order to fulfill SC-7, an organization would need to implement ECND.

(PEVC "Visitor Control to Computing Facilities" is unusual in that it spans more than one 800-53 control. PEVC calls for procedures for visitor access and logs of those visits. PE-7 "Visitor Control" covers the former and PE-8 "Access Records" the latter.)

[30] This is Table 1-1, page 6, of NIST 800-53, augmented with the two rightmost columns.

[31] This column is central to the next section of this report and is included here to provide a mapping to the families.

[32] This column shows the sum of the controls in the respective NIST family and does not refer to 8500.2 IACs.

[33] "SA" is the identifier for the "System and Services Acquisition" family.

Identifier	Family	Class[31]	Controls[32]	Matching ICGs from 8500.2
MP	Media Protection	Operational	6	4
PE	Physical and Environmental Protection	Operational	19	16
PL	Planning	Management	5	4
PS	Personnel Security	Operational	8	2
RA	Risk Assessment	Management	4	1
SA	System and Services Acquisition	Management	14	8
SC	System and Communications Protection	Technical	34	15
SI	System and Information Integrity	Operational	13	3
PM[34]	Program Management	Management	11	1
TOTAL	18		198	109

The ICGs cover all 18 of the NIST families and 43% of the ICGs are concentrated in three families, as noted above:

- Access Control (AC),
- Physical & Environmental Protection (PE), and
- System & Communication Protection (SC)

This suggests that these areas are the highest concern to 8500.2. Meanwhile, most of the ICGs in the AC and SC (as well as AU) NIST families are from the 8500.2 EC subject area. Most of the ICGs in the PE NIST family are naturally from the 8500.2 PE subject area.

The next table shows the mapping for each ICG.

Table 35 ICG-to-NIST Mapping

#	ICG	NIST Family Name	NIST Control Name	NIST Control
1	ECNK	System and Communications Protection	Transmission Confidentiality	SC-9
2	ECCR	System and Communications Protection	Protection of Information at Rest	SC-28
3	ECCT	System and Communications Protection	Transmission Confidentiality	SC-9
4	ECLO	Access Control	Unsuccessful Login Attempts	AC-7

[34] PM and its controls look like a family and they are listed as a family in Table 1-1 but they are shown in their own Appendix (Appendix G) of 800-53, not Appendix F where all of the other families are listed. Perhaps we could say that PM is a different kind of family.

#	ICG	NIST Family Name	NIST Control Name	NIST Control
5	IAIA	Identification and Authentication	Authenticator Management	IA-5
6	PECF	Physical and Environmental Protection	Physical Access Authorizations	PE-2
7	PECS	Media Protection	Media Sanitization	MP-6
8	PEPF	Physical and Environmental Protection	Physical Access Control	PE-3
9	PRAS	Personnel Security	Personnel Screening	PS-3
10	EBPW	System and Communications Protection	Boundary Protection	SC-7
11	ECCM	System and Communications Protection	Cryptographic Key Establishment and Management	SC-12
12	ECLC	Audit and Accountability	Content of Audit Records	AU-3
13	PEDD	Media Protection	Media Sanitization	MP-6
14	EBRP	Access Control	Remote Access	AC-17
15	EBRU	Access Control	Remote Access	AC-17
16	ECAD	Access Control	Access Enforcement	AC-3
17	ECAN	Access Control	Access Enforcement	AC-3
18	ECIC	Access Control	Information Flow Enforcement	AC-4
19	ECML	Media Protection	Media Marking	MP-3
20	ECRC	System and Communications Protection	Information in Shared Resources	SC-4
21	ECTC	Physical and Environmental Protection	Information Leakage	PE-19
22	IAAC	Access Control	Account Management	AC-2
23	IAGA	Identification and Authentication	Identification and Authentication (Organizational Users)	IA-2
24	PEDI	Physical and Environmental Protection	Access Control for Output Devices	PE-5
25	PEPS	Physical and Environmental Protection	Physical Access Control	PE-3
26	PESP	Planning	Rules of Behavior	PL-4
27	PESS	Media Protection	Media Storage	MP-4
28	PEVC	Physical and Environmental Protection	Visitor Control	PE-7+8
29	PRTN	Awareness and Training	Security Training	AT-3
30	DCPA	System and Communications Protection	Application Partitioning	SC-2
31	DCPB	System and Services Acquisition	Allocation of Resources	SA-2
32	DCSP	System and Communications Protection	Security Function Isolation	SC-3
33	ECDC	Contingency Planning	Information System Recovery and Reconstitution	CP-10

#	ICG	NIST Family Name	NIST Control Name	NIST Control
34	ECID	System and Information Security	Information System Monitoring	SI-4
35	ECTB	Audit and Accountability	Protection of Audit Information	AU-9
36	ECMT	Security Assessment and Authorization	Continuous Monitoring	CA-7
37	PRMP	Maintenance	Maintenance Personnel	MA-5
38	DCSR	System and Services Acquisition	Critical Information System Components	SA-14
39	EBBD	System and Communications Protection	Boundary Protection	SC-7
40	ECAR	Audit and Accountability	Content of Audit Records	AU-3
41	COEB	Physical and Environmental Protection	Alternate Work Site	PE-17
42	COED	Contingency Planning	Contingency Plan Testing and Exercises	CP-4
43	COSP	Maintenance	Timely Maintenance	MA-6
44	VIIR	Incident Response	Incident Response Plan	IR-8
45	COAS	Contingency Planning	Alternate Processing Site	CP-7
46	COEF	Contingency Planning	Contingency Plan	CP-2
47	COMS	Maintenance	Timely Maintenance	MA-6
48	DCCB	Configuration Management	Configuration Change Control	CM-3
49	DCCS	Configuration Management	Configuration Settings	CM-6
50	ECND	System and Communications Protection	Boundary Protection	SC-7
51	ECPC	Access Control	Account Management	AC-2
52	ECSD	Configuration Management	Access Restrictions for Change	CM-5
53	ECTM	System and Communications Protection	Transmission Integrity	SC-8
54	IATS	Identification and Authentication	Authenticator Management	IA-5
55	PEEL	Physical and Environmental Protection	Emergency Lighting	PE-12
56	PEFD	Physical and Environmental Protection	Fire Protection	PE-13
57	PEFS	Physical and Environmental Protection	Fire Protection	PE-13
58	PEHC	Physical and Environmental Protection	Temperature and Humidity Controls	PE-14
59	PETC	Physical and Environmental Protection	Temperature and Humidity Controls	PE-14
60	DCSS	System and Communications Protection	Fail in Known State	SC-24
61	ECCD	Access Control	Access Enforcement	AC-3
62	ECAT	Audit and Accountability	Audit Review, Analysis, and Reporting	AU-6

#	ICG	NIST Family Name	NIST Control Name	NIST Control
63	IAKM	System and Communications Protection	Cryptographic Key Establishment and Management	SC-12
64	CODB	Contingency Planning	Information System Backup	CP-9
65	CODP	Contingency Planning	Contingency Plan	CP-2
66	COPS	Physical and Environmental Protection	Emergency Power	PE-11
67	DCAS	System and Services Acquisition	Acquisitions	SA-4
68	ECLP	Access Control	Least Privilege	AC-6
69	ECRR	Audit and Accountability	Audit Record Retention	AU-11
70	ECWM	Access Control	System Use Notification	AC-8
71	PRNK	Personnel Security	Personnel Screening	PS-3
72	COBR	Contingency Planning	Information System Backup	CP-9
73	COSW	Contingency Planning	Alternate Site Storage	CP-6
74	COTR	Contingency Planning	Information System Recovery and Reconstitution	CP-10
75	DCAR	Planning	System Security Plan	PL-2
76	DCBP	Identification and Authentication	Authenticator Management	IA-5
77	DCCT	System and Services Acquisition	Developer Security Training	SA-11
78	DCDS	System and Services Acquisition	External Information System Services	SA-9
79	DCFA	Program Management	Enterprise Architecture	PL-2
80	DCHW	Configuration Management	Information System Component Inventory	CM-8
81	DCID	Security Assessment and Authorization	Information System Connections	CA-3
82	DCII	Configuration Management	Security Impact Analysis	CM-4
83	DCIT	System and Services Acquisition	External Information System Services	SA-9
84	DCMC	System and Communications Protection	Mobile Code	SC-18
85	DCNR	Audit and Accountability	Non-repudiation	AU-10
86	DCPD	System and Services Acquisition	Software Usage Restrictions	SA-6
87	DCPP	Security Assessment and Authorization	Information System Connections	CA-3
88	DCPR	Configuration Management	Configuration Management Plan	CM-9
89	DCSD	Planning	System Security Plan	PL-2
90	DCSL	Configuration Management	Access Restrictions for Change	CM-5
91	DCSQ	System and Services Acquisition	Developer Security Training	SA-11
92	DCSW	Configuration Management	Information System Component	CM-8

#	ICG	NIST Family Name	NIST Control Name	NIST Control
			Inventory	
93	EBCR	Access Control	Information Flow Enforcement	AC-4
94	EBVC	System and Information Security	Information System Monitoring	SI-4
95	ECIM	Access Control	Information Flow Enforcement	AC-4
96	ECPA	Access Control	Account Management	AC-2
97	ECRG	Audit and Accountability	Audit Reduction and Report Generation	AU-7
98	ECSC	Configuration Management	Configuration Settings	CM-6
99	ECTP	Audit and Accountability	Protection of Audit Information	AU-9
100	ECVI	System and Communications Protection	Voice Over Internet Protocol	SC-19
101	ECVP	System and Information Security	Malicious Code Protection	SI-3
102	ECWN	Access Control	Wireless Access	AC-18
103	PEFI	Physical and Environmental Protection	Fire Protection	PE-13
104	PEMS	Physical and Environmental Protection	Emergency Shutoff	PE-10
105	PESL	Access Control	Session Lock	AC-11
106	PETN	Awareness and Training	Security Training	AT-3
107	PEVR	Physical and Environmental Protection	Power Equipment and Power Cabling	PE-9
108	PRRB	Planning	Rules of Behavior	PL-4
109	VIVM	Risk Assessment	Vulnerability Scanning	RA-5

The partition table, sorted on Family, is shown below.

Table 36 Partition Table, Sorted on Family

#	ICG	Signature	Type	CIA	Span	Impact	Family	Class	Coverage
105	PESL	111---	3	I	1	C	AC-11	T	DS5.4
14	EBRP	---11-	1	C	1	A	AC-17	T	DS5.10
15	EBRU	---11-	1	C	1	A	AC-17	T	DS5.10
102	ECWN	111---	3	A	1	A	AC-18	T	DS5.10
22	IAAC	---11-	1	C	1	A	AC-2	T	DS5.4
51	ECPC	221---	2	I	2	C	AC-2	T	DS5.4
96	ECPA	111---	3	I	1	A	AC-2	T	DS5.4
16	ECAD	---11-	1	C	1	C	AC-3	T	DS5.3
17	ECAN	---11-	1	C	1	A	AC-3	T	DS5.4
61	ECCD	2212--	2	I	2	B	AC-3	T	DS11.6
18	ECIC	---11-	1	C	1	C	AC-4	T	DS5.10
93	EBCR	111---	3	A	1	C	AC-4	T	DS5.10
95	ECIM	111---	3	I	1	C	AC-4	T	DS5.10
68	ECLP	---111	3	C	1	A	AC-6	T	DS5.4

#	ICG	Signature	Type	CIA	Span	Impact	Family	Class	Coverage
4	ECLO	---21-	0	C	2	C	AC-7	T	DS5.4
70	ECWM	---111	3	C	1	E	AC-8	T	DS5.7
29	PRTN	---11-	1	I	1	A	AT-3	O	DS7.2
106	PETN	111---	3	A	1	E	AT-3	O	DS7.2
85	DCNR	111---	3	I	1	C	AU-10	T	DS5.8
69	ECRR	---111	3	I	1	C	AU-11	T	DS5.5
12	ECLC	---1--	1	C	1	E	AU-3	T	DS5.5
40	ECAR	---321	2	ICC	3	Z	AU-3	T	DS5.5
62	ECAT	221211	2	I	2	D	AU-6	T	DS5.5
97	ECRG	111---	3	I	1	E	AU-7	T	DS5.5
35	ECTB	11-1--	1	I	1	C	AU-9	T	DS11.5
99	ECTP	111---	3	I	1	C	AU-9	T	DS11.6
81	DCID	111---	3	I	1	A	CA-3	M	DS5.10
87	DCPP	111---	3	A	1	C	CA-3	M	DS5.10
36	ECMT	---211	2	C	2	D	CA-7	M	ME2.4
48	DCCB	221---	2	I	2	D	CM-3	O	DS9
82	DCII	111---	3	I	1	C	CM-4	O	AI6.2
52	ECSD	221---	2	I	2	B	CM-5	O	DS11.3
90	DCSL	111---	3	I	1	C	CM-5	O	DS11.3
49	DCCS	221---	2	I	2	A	CM-6	O	DS9.1
98	ECSC	111---	3	A	1	A	CM-6	O	AI2.5
80	DCHW	111---	3	A	1	A	CM-8	O	DS9.2
92	DCSW	111---	3	A	1	A	CM-8	O	DS9.2
88	DCPR	111---	3	I	1	A	CM-9	O	DS9
33	ECDC	11----	1	I	1	C	CP-10	O	DS11.6
74	COTR	111---	3	A	1	A	CP-10	O	DS4.8
46	COEF	221---	2	A	2	D	CP-2	O	DS4.2
65	CODP	321---	2	A	3	D	CP-2	O	DS4.2
42	COED	211---	2	A	2	D	CP-4	O	DS4.5
73	COSW	111---	3	A	1	A	CP-6	O	DS4.9
45	COAS	221---	2	A	2	B	CP-7	O	DS4.2
64	CODB	321---	2	A	3	D	CP-9	O	DS11.5
72	COBR	111---	3	A	1	A	CP-9	O	DS11.6
23	IAGA	---11-	1	C	1	C	IA-2	T	DS5.4
5	IAIA	---21-	0	C	2	A	IA-5	T	DS5.4
54	IATS	221---	2	I	2	C	IA-5	T	DS5.8
76	DCBP	111---	3	I	1	C	IA-5	T	DS5.4
44	VIIR	211---	2	A	2	B	IR-8	O	DS8
37	PRMP	---211	2	C	2	A	MA-5	O	DS1.3
43	COSP	211---	2	A	2	D	MA-6	O	DS1.3
47	COMS	221---	2	A	2	D	MA-6	O	DS1.3
19	ECML	---11-	1	C	1	A	MP-3	O	DS11.6
27	PESS	---11-	1	C	1	A	MP-4	O	DS11.2
7	PECS	---21-	0	C	2	A	MP-6	O	DS5.11

#	ICG	Signature	Type	CIA	Span	Impact	Family	Class	Coverage
13	PEDD	---1--	1	C	1	A	MP-6	O	DS11.4
104	PEMS	111---	3	A	1	A	PE-10	O	DS12.4
66	COPS	321---	2	A	3	D	PE-11	O	DS12.4
55	PEEL	221---	2	A	2	D	PE-12	O	DS12.4
56	PEFD	221---	2	A	2	A	PE-13	O	DS12.4
57	PEFS	221---	2	A	2	B	PE-13	O	DS12.4
103	PEFI	111---	3	A	1	C	PE-13	O	DS12.4
58	PEHC	221---	2	A	2	C	PE-14	O	DS12.4
59	PETC	221---	2	A	2	D	PE-14	O	DS12.4
41	COEB	211---	2	A	2	B	PE-17	O	DS4.2
21	ECTC	---11-	1	C	1	A	PE-19	O	DS5.5
6	PECF	---21-	0	C	2	A	PE-2	O	DS12.3
8	PEPF	---21-	0	C	2	A	PE-3	O	DS12.3
25	PEPS	---11-	1	C	1	E	PE-3	O	DS12.2
24	PEDI	---11-	1	C	1	A	PE-5	O	DS11.6
28	PEVC	---11-	1	C	1	A	PE-7+8	O	DS12.3
107	PEVR	111---	3	A	1	A	PE-9	O	DS12.4
75	DCAR	111---	3	A	1	C	PL-2	M	DS5.2
79	DCFA	111---	3	I	1	C	PL-2	M	PO2.1
89	DCSD	111---	3	A	1	A	PL-2	M	DS5.2
26	PESP	---11-	1	C	1	C	PL-4	M	DS11.6
108	PRRB	111---	3	A	1	A	PL-4	M	DS5.2
9	PRAS	---21-	0	C	2	A	PS-3	O	DS5.4
71	PRNK	---111	3	C	1	A	PS-3	O	DS5.4
109	VIVM	111---	3	A	1	C	RA-5	M	DS5.2
77	DCCT	111---	3	A	1	C	SA-11	M	AI6.2
91	DCSQ	111---	3	I	1	C	SA-11	M	AI2.8
38	DCSR	---321	2	C	3	A	SA-14	M	DS5.2
31	DCPB	11----	1	A	1	A	SA-2	M	PO5.1
67	DCAS	---111	3	C	1	A	SA-4	M	AI5.3
86	DCPD	111---	3	A	1	C	SA-6	M	AI5.3
78	DCDS	111---	3	I	1	C	SA-9	M	DS2.3
83	DCIT	111---	3	I	1	A	SA-9	M	DS1.3
11	ECCM	---1--	1	C	1	A	SC-12	T	DS5.8
63	IAKM	2213--	2	I	3	C	SC-12	T	DS5.8
84	DCMC	111---	3	I	1	C	SC-18	T	DS5.9
100	ECVI	111---	3	A	1	C	SC-19	T	DS5.10
30	DCPA	11----	1	I	1	E	SC-2	T	DS11.6
60	DCSS	2212--	2	I	2	A	SC-24	T	AI2.4
2	ECCR	---2+31-	0	C	2	Z	SC-28	T	DS11.6
32	DCSP	11----	1	I	1	C	SC-3	T	DS5.7
20	ECRC	---11-	1	C	1	C	SC-4	T	DS11.6
10	EBPW	----11	1	C	1	A	SC-7	T	DS5.10
39	EBBD	---321	2	C	3	Z	SC-7	T	DS5.10

#	ICG	Signature	Type	CIA	Span	Impact	Family	Class	Coverage
50	ECND	221---	2	I	2	D	SC-7	T	DS5.10
53	ECTM	221---	2	I	2	C	SC-8	T	DS5.11
1	ECNK	---1+21-	0	C	2	C	SC-9	T	DS5.11
3	ECCT	---21-	0	C	2	B	SC-9	T	DS5.11
101	ECVP	111---	3	A	1	A	SI-3	O	DS5.9
34	ECID	11----	1	I	1	C	SI-4	O	DS5.9
94	EBVC	111---	3	A	1	C	SI-4	O	DS5.10

3.6 Class

This section explores the concept of "class" for ICGs using the class for corresponding 800-53 families, as introduced in the previous section.

A given ICG's class tells us

- who is responsible for implementing compliance,
- who is responsible for maintaining the compliance, and
- to whom we should go when we audit compliance.

800-53 [10] partitions its families based on what it calls their "class." Based on FIPS 200 [7], 800-53 provides explicit definitions for the three elements—management, operational, and technical—as shown below.

> Management Controls
>
> > The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security. (800-53, page B-7 (and FIPS 200, page 7))
>
> Operational Controls
>
> > The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems). (800-53, page B-9 (and FIPS 200, page 8))
>
> Technical Controls
>
> > The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. (800-53, page B-15 (and FIPS 200, page 9))

Management is responsible for Management controls; operations is responsible for Operational controls; and technicians are responsible for Technical controls.

8500.2 does not indicate the class to which each ICG belongs. However, 800-53 has partitioned its controls such that all the controls in each family are of the same class. In the previous section of this report each of the ICGs were matched to a family in 800-53. So, for a given ICG, we can infer what its class should be by determining the 800-53 family to which the ICG is mapped. (This presumes, of course, that the mapping in the previous section is correct.) Accordingly, using the table from the previous section we determine that there are 17, 49, and 43 ICGs in the Management, Operational, and Technical classes, respectively, as shown in the next table.

Table 37 Class Breakdown

Class	ICGs	Percentage
Management	17	16%
Operational	49	45%
Technical	43	39%
TOTAL	109	100%

We expect that the ICGs would be evenly distributed across the three Classes—that 1/3 (about 36) of the ICGs would be in each class. However, the Classes are weighted heavily toward Operational and slightly toward Technical, with the Management class less than half of what we expect. This only means that the ICGs provide the most detail for operations: operations has the longest list of items to attend to while management has the shortest list. This does not necessarily reflect relative importance.

The partition table, sorted on Class, is shown below.

Table 38 Partition Table, Sorted on Class

#	ICG	Signature	Type	CIA	Span	Impact	Family	Class	Coverage
26	PESP	---11-	1	C	1	C	PL-4	M	DS11.6
31	DCPB	11----	1	A	1	A	SA-2	M	PO5.1
36	ECMT	---211	2	C	2	D	CA-7	M	ME2.4
38	DCSR	---321	2	C	3	A	SA-14	M	DS5.2
67	DCAS	---111	3	C	1	A	SA-4	M	AI5.3
75	DCAR	111---	3	A	1	C	PL-2	M	DS5.2
77	DCCT	111---	3	A	1	C	SA-11	M	AI6.2
78	DCDS	111---	3	I	1	C	SA-9	M	DS2.3
79	DCFA	111---	3	I	1	C	PL-2	M	PO2.1
81	DCID	111---	3	I	1	A	CA-3	M	DS5.10
83	DCIT	111---	3	I	1	A	SA-9	M	DS1.3
86	DCPD	111---	3	A	1	C	SA-6	M	AI5.3
87	DCPP	111---	3	A	1	C	CA-3	M	DS5.10
89	DCSD	111---	3	A	1	A	PL-2	M	DS5.2
91	DCSQ	111---	3	I	1	C	SA-11	M	AI2.8
108	PRRB	111---	3	A	1	A	PL-4	M	DS5.2
109	VIVM	111---	3	A	1	C	RA-5	M	DS5.2
6	PECF	---21-	0	C	2	A	PE-2	O	DS12.3
7	PECS	---21-	0	C	2	A	MP-6	O	DS5.11
8	PEPF	---21-	0	C	2	A	PE-3	O	DS12.3
9	PRAS	---21-	0	C	2	A	PS-3	O	DS5.4
13	PEDD	---1--	1	C	1	A	MP-6	O	DS11.4
19	ECML	---11-	1	C	1	A	MP-3	O	DS11.6
21	ECTC	---11-	1	C	1	A	PE-19	O	DS5.5
24	PEDI	---11-	1	C	1	A	PE-5	O	DS11.6
25	PEPS	---11-	1	C	1	E	PE-3	O	DS12.2
27	PESS	---11-	1	C	1	A	MP-4	O	DS11.2
28	PEVC	---11-	1	C	1	A	PE-7+8	O	DS12.3

#	ICG	Signature	Type	CIA	Span	Impact	Family	Class	Coverage
29	PRTN	---11-	1	I	1	A	AT-3	O	DS7.2
33	ECDC	11----	1	I	1	C	CP-10	O	DS11.6
34	ECID	11----	1	I	1	C	SI-4	O	DS5.9
37	PRMP	---211	2	C	2	A	MA-5	O	DS1.3
41	COEB	211---	2	A	2	B	PE-17	O	DS4.2
42	COED	211---	2	A	2	D	CP-4	O	DS4.5
43	COSP	211---	2	A	2	D	MA-6	O	DS1.3
44	VIIR	211---	2	A	2	B	IR-8	O	DS8
45	COAS	221---	2	A	2	B	CP-7	O	DS4.2
46	COEF	221---	2	A	2	D	CP-2	O	DS4.2
47	COMS	221---	2	A	2	D	MA-6	O	DS1.3
48	DCCB	221---	2	I	2	D	CM-3	O	DS9
49	DCCS	221---	2	I	2	A	CM-6	O	DS9.1
52	ECSD	221---	2	I	2	B	CM-5	O	DS11.3
55	PEEL	221---	2	A	2	D	PE-12	O	DS12.4
56	PEFD	221---	2	A	2	A	PE-13	O	DS12.4
57	PEFS	221---	2	A	2	B	PE-13	O	DS12.4
58	PEHC	221---	2	A	2	C	PE-14	O	DS12.4
59	PETC	221---	2	A	2	D	PE-14	O	DS12.4
64	CODB	321---	2	A	3	D	CP-9	O	DS11.5
65	CODP	321---	2	A	3	D	CP-2	O	DS4.2
66	COPS	321---	2	A	3	D	PE-11	O	DS12.4
71	PRNK	---111	3	C	1	A	PS-3	O	DS5.4
72	COBR	111---	3	A	1	A	CP-9	O	DS11.6
73	COSW	111---	3	A	1	A	CP-6	O	DS4.9
74	COTR	111---	3	A	1	A	CP-10	O	DS4.8
80	DCHW	111---	3	A	1	A	CM-8	O	DS9.2
82	DCII	111---	3	I	1	C	CM-4	O	AI6.2
88	DCPR	111---	3	I	1	A	CM-9	O	DS9
90	DCSL	111---	3	I	1	C	CM-5	O	DS11.3
92	DCSW	111---	3	A	1	A	CM-8	O	DS9.2
94	EBVC	111---	3	A	1	C	SI-4	O	DS5.10
98	ECSC	111---	3	A	1	A	CM-6	O	AI2.5
101	ECVP	111---	3	A	1	A	SI-3	O	DS5.9
103	PEFI	111---	3	A	1	C	PE-13	O	DS12.4
104	PEMS	111---	3	A	1	A	PE-10	O	DS12.4
106	PETN	111---	3	A	1	E	AT-3	O	DS7.2
107	PEVR	111---	3	A	1	A	PE-9	O	DS12.4
1	ECNK	---1+21-	0	C	2	C	SC-9	T	DS5.11
2	ECCR	---2+31-	0	C	2	Z	SC-28	T	DS11.6
3	ECCT	---21-	0	C	2	B	SC-9	T	DS5.11
4	ECLO	---21-	0	C	2	C	AC-7	T	DS5.4
5	IAIA	---21-	0	C	2	A	IA-5	T	DS5.4
10	EBPW	----11	1	C	1	A	SC-7	T	DS5.10

#	ICG	Signature	Type	CIA	Span	Impact	Family	Class	Coverage
11	ECCM	---1--	1	C	1	A	SC-12	T	DS5.8
12	ECLC	---1--	1	C	1	E	AU-3	T	DS5.5
14	EBRP	---11-	1	C	1	A	AC-17	T	DS5.10
15	EBRU	---11-	1	C	1	A	AC-17	T	DS5.10
16	ECAD	---11-	1	C	1	C	AC-3	T	DS5.3
17	ECAN	---11-	1	C	1	A	AC-3	T	DS5.4
18	ECIC	---11-	1	C	1	C	AC-4	T	DS5.10
20	ECRC	---11-	1	C	1	C	SC-4	T	DS11.6
22	IAAC	---11-	1	C	1	A	AC-2	T	DS5.4
23	IAGA	---11-	1	C	1	C	IA-2	T	DS5.4
30	DCPA	11----	1	I	1	E	SC-2	T	DS11.6
32	DCSP	11----	1	I	1	C	SC-3	T	DS5.7
35	ECTB	11-1--	1	I	1	C	AU-9	T	DS11.5
39	EBBD	---321	2	C	3	Z	SC-7	T	DS5.10
40	ECAR	---321	2	ICC	3	Z	AU-3	T	DS5.5
50	ECND	221---	2	I	2	D	SC-7	T	DS5.10
51	ECPC	221---	2	I	2	C	AC-2	T	DS5.4
53	ECTM	221---	2	I	2	C	SC-8	T	DS5.11
54	IATS	221---	2	I	2	C	IA-5	T	DS5.8
60	DCSS	2212--	2	I	2	A	SC-24	T	AI2.4
61	ECCD	2212--	2	I	2	B	AC-3	T	DS11.6
62	ECAT	221211	2	I	2	D	AU-6	T	DS5.5
63	IAKM	2213--	2	I	3	C	SC-12	T	DS5.8
68	ECLP	---111	3	C	1	A	AC-6	T	DS5.4
69	ECRR	---111	3	I	1	C	AU-11	T	DS5.5
70	ECWM	---111	3	C	1	E	AC-8	T	DS5.7
76	DCBP	111---	3	I	1	C	IA-5	T	DS5.4
84	DCMC	111---	3	I	1	C	SC-18	T	DS5.9
85	DCNR	111---	3	I	1	C	AU-10	T	DS5.8
93	EBCR	111---	3	A	1	C	AC-4	T	DS5.10
95	ECIM	111---	3	I	1	C	AC-4	T	DS5.10
96	ECPA	111---	3	I	1	A	AC-2	T	DS5.4
97	ECRG	111---	3	I	1	E	AU-7	T	DS5.5
99	ECTP	111---	3	I	1	C	AU-9	T	DS11.6
100	ECVI	111---	3	A	1	C	SC-19	T	DS5.10
102	ECWN	111---	3	A	1	A	AC-18	T	DS5.10
105	PESL	111---	3	I	1	C	AC-11	T	DS5.4

3.7 Coverage

This section explores the extent of coverage by the ICGs. That is, this section answers the questions, "What do the ICGs focus on? and what do the ICGs leave for some other controls outside of 8500.2?" We saw some of this in the section above on NIST 800-53 "families." This section provides more depth.

In order to answer these questions we need a control set that has great breadth. The control set of which we are aware that has the greatest breadth is the Control Objectives for IT and Related Technology (COBIT) [1] from the IT Governance Institute (ITGI) [9]. ITGI began in 1998 as a research extension of ISACA [8], which was and continues to be the new name for the EDP Auditors Foundation, established in the 1960's. Until a few years ago, "ISACA" was an acronym for "Information Systems Audit and Control Association," but the organization wanted to be confined no longer to auditing: its set of controls, namely COBIT, had expanded into the larger arena of "IT governance." ISACA is thus now a name and no longer an acronym.

The intent of COBIT is to span the IT governance spectrum, which spectrum is larger than 800-53 and larger still than 8500.2. While Herrmann is correct in pointing out that the term "governance," is a synonym for "management" ([2], page 132), the term "IT management," by customary usage, implies the scope of what we called in the previous section the "Management Controls." IT governance, on the other hand, is intended to describe all of the management responsibilities for IT. In order to convey that larger scope a new term is needed, or else much time is wasted in the confusion caused by using one term for multiple meanings.

COBIT has a four-tiered structure with

1. 4 "domains" which consist of…
2. 34 "processes" which consist of…
3. 210 "control objectives" which consist of…
4. approximately 1600 "control practice statements."[35]

COBIT's structure is shown in the next table.

Table 39 COBIT Structure

Level	Name	Items
1	Domain	4
2	Process	34
3	Control Objective	210
4	Control Practice Statement	Approximately 1600

[35] Where "practice" has the same meaning as in the expression "best practice" and not as in practice vs. performance.

Similar to the way this report mapped the ICGs to the families in 800-53, as shown in a previous section, this section maps the ICGs to the domains, processes, and control objectives in COBIT.[36] As we will see, the ICGs have a narrow scope, focusing on what COBIT calls system security. Almost all of the ICGs fall within one Domain (namely Deliver and Support (DS)), and half of those ICGs in turn fall within one Process (namely DS5 "Ensure systems security"), and half of those ICGs in turn fall within two Control Objectives (namely, DS5.4 "User account management" and DS5.10 "Network security").

The next table shows the number of ICGs in each Domain of COBIT. (Note that, like the mapping of ICGs to 800-53 families, presented in Table 34 on page 65 above, the mapping shown here has been generated for this report and has unavoidably some subjectivity.) At the Domain level the results indicate that the ICGs focus almost exclusively on the "Deliver and Support" Domain.

Table 40 Mapping ICGs to the COBIT Domains

Domain	Mapped ICGs	Percentage of ICGs
Plan and Organise[37] (PO)	2	2%
Acquire and Implement (AI)	7	7%
Deliver and Support (DS)	99	91%
Monitor and Evaluate (ME)	1	1%
TOTAL	109	100%

At the Process level the ICGs focus on the DS5 "Ensure system security" Process, as shown in the next table. In order to grasp the extent of each Process, the next table also shows the number of Control Objectives in each Process.

Table 41 Mapping ICGs to COBIT Domains and Processes

Domain	Process	Control Objectives	Mapped ICGs
Plan and Organise (PO)	PO1 Define a strategic IT Plan	6	
	PO2 Define the information architecture	4	1
	PO3 Determine technological direction	5	
	PO4 Define the IT process, organisation and relationships	15	
	PO5 Manage the IT investment	5	1
	PO6 Communicate management aims and direction	5	
	PO7 Manage IT human resources	8	
	PO8 Manage quality	6	
	PO9 Assess and manage IT risks	6	
	PO10 Manage Projects	14	

[36] The control practice statements are too fine grained for useful mapping.

[37] The European spelling—"s" here instead of "z"—is used throughout COBIT.

Domain	Process	Control Objectives	Mapped ICGs
Acquire and Implement (AI)	AI1 Identify automated solutions	4	
	AI2 Acquire and maintain application software	10	3
	AI3 Acquire and maintain technology infrastructure	4	
	AI4 Enable operation and use	4	
	AI5 Procure IT resources	4	2
	AI6 Manage changes	5	2
	AI7 Install and accredit solutions and changes	9	
Deliver and Support (DS)	DS1 Define and manager service levels	6	4
	DS2 Manage third-party services	4	1
	DS3 Manage performance and capacity	5	
	DS4 Ensure continuous service	10	7
	DS5 Ensure systems security	11	51
	DS6 Identify and allocate costs	4	
	DS7 Educate and train users	3	2
	DS8 Manage service desk and incidents	5	1
	DS9 Manage the configuration	3	5
	DS10 Manage problems	4	
	DS11 Manage data	6	16
	DS12 Manage the physical environment	5	13
	DS13 Manage operations	5	
Monitor and Evaluate (ME)	ME1 Monitor and evaluate IT performance	6	
	ME2 Monitor and evaluate internal control	7	1
	ME3 Ensure compliance with external requirements	5	
	ME4 Provide IT governance	7	
TOTAL		210	109

At the Control Objective level, within the DS5 "Ensure system security" Process, the results indicate that the ICGs focus on two Control Objectives:

- DS5.4 "User account management" and
- DS5.10 "Network security"

with 12 and 13 ICGs, respectively, in each. A third Control Objective, DS5.5 "Security testing, surveillance and monitoring," trails with 6 ICGs. These three Control Objectives account for 31 (i.e., 2/3) of the 51 ICGs that fall within the DS5 Process, as shown in the next table.

Table 42 Mapping ICGs to COBIT Process DS5

Control Objective	Name	Mapped ICGs	% of 51 ICGs
DS5.1	Management of IT security		
DS5.2	IT security plan	5	10
DS5.3	Identity management	1	2
DS5.4	User account management	12	26
DS5.5	Security testing, surveillance and monitoring	6	16
DS5.6	Security incident definition		
DS5.7	Protection of security technology	2	4
DS5.8	Cryptographic key management	4	8
DS5.9	Malicious software prevention, detection and correction	3	2
DS5.10	Network security	13	26
DS5.11	Exchange of sensitive data	4	8
TOTAL		51	100

The next table shows the mapping for each ICG.

Table 43 ICG-to-COBIT Mapping

#	ICG	COBIT Process Name	COBIT Control Objective Name	COBIT Control Objective
1	ECNK	Ensure systems security	Exchange of sensitive data	DS5.11
2	ECCR	Manage data	Security Requirements for data management	DS11.6
3	ECCT	Ensure systems security	Exchange of sensitive data	DS5.11
4	ECLO	Ensure systems security	User account management	DS5.4
5	IAIA	Ensure systems security	User account management	DS5.4
6	PECF	Manage the physical environment	Physical access	DS12.3
7	PECS	Ensure systems security	Exchange of sensitive data	DS5.11
8	PEPF	Manage the physical environment	Physical access	DS12.3
9	PRAS	Ensure systems security	User account management	DS5.4
10	EBPW	Ensure systems security	Network security	DS5.10
11	ECCM	Ensure systems security	Cryptographic key management	DS5.8
12	ECLC	Ensure systems security	Security testing, surveillance and monitoring	DS5.5
13	PEDD	Manage data	Disposal	DS11.4
14	EBRP	Ensure systems security	Network security	DS5.10
15	EBRU	Ensure systems security	Network security	DS5.10
16	ECAD	Ensure systems security	Identify management	DS5.3
17	ECAN	Ensure systems security	User account management	DS5.4
18	ECIC	Ensure systems security	Network security	DS5.10
19	ECML	Manage data	Security Requirements for data	DS11.6

#	ICG	COBIT Process Name	COBIT Control Objective Name	COBIT Control Objective
			management	
20	ECRC	Manage data	Security Requirements for data management	DS11.6
21	ECTC	Ensure systems security	Security testing, surveillance and monitoring	DS5.5
22	IAAC	Ensure systems security	User account management	DS5.4
23	IAGA	Ensure systems security	User account management	DS5.4
24	PEDI	Manage data	Security requirements for data management	DS11.6
25	PEPS	Manage the physical environment	Physical security measures	DS12.2
26	PESP	Manage data	Security requirements for data management	DS11.6
27	PESS	Manage data	Storage and retention arrangements	DS11.2
28	PEVC	Manage the physical environment	Physical access	DS12.3
29	PRTN	Educate and train users	Delivery of training and education	DS7.2
30	DCPA	Manage data	Security requirements for data management	DS11.6
31	DCPB	Manage the IT investment	Financial management framework	PO5.1
32	DCSP	Ensure systems security	Protection of security technology	DS5.7
33	ECDC	Manage data	Security requirements for data management	DS11.6
34	ECID	Ensure systems security	Malicious software prevention, detection and correction	DS5.9
35	ECTB	Manage data	Backup and restoration	DS11.5
36	ECMT	Monitor and evaluate internal control	Control self-assessment	ME2.4
37	PRMP	Define and manage service levels	Service level agreements	DS1.3
38	DCSR	Ensure systems security	IT security plan	DS5.2
39	EBBD	Ensure systems security	Network security	DS5.10
40	ECAR	Ensure systems security	Security testing, surveillance and monitoring	DS5.5
41	COEB	Ensure continuous service	IT continuity plans	DS4.2
42	COED	Ensure continuous service	Testing of the IT continuity plan	DS4.5
43	COSP	Define and manage service levels	Service level agreements	DS1.3
44	VIIR	Manage service desk and incidents	(The ICG covers most of the process)	DS8

#	ICG	COBIT Process Name	COBIT Control Objective Name	COBIT Control Objective
45	COAS	Ensure continuous service	IT continuity plans	DS4.2
46	COEF	Ensure continuous service	IT continuity plans	DS4.2
47	COMS	Define and manage service levels	Service level agreements	DS1.3
48	DCCB	Manage the configuration	(The ICG covers most of the process)	DS9
49	DCCS	Manage the configuration	Configuration repository and baseline	DS9.1
50	ECND	Ensure systems security	Network security	DS5.10
51	ECPC	Ensure systems security	User account management	DS5.4
52	ECSD	Manage data	Media library management system	DS11.3
53	ECTM	Ensure systems security	Exchange of sensitive data	DS5.11
54	IATS	Ensure systems security	Cryptographic key management	DS5.8
55	PEEL	Manage the physical environment	Protection against environmental factors	DS12.4
56	PEFD	Manage the physical environment	Protection against environmental factors	DS12.4
57	PEFS	Manage the physical environment	Protection against environmental factors	DS12.4
58	PEHC	Manage the physical environment	Protection against environmental factors	DS12.4
59	PETC	Manage the physical environment	Protection against environmental factors	DS12.4
60	DCSS	Acquire and maintain application software	Application security and availability	AI2.4
61	ECCD	Manage data	Security requirements for data management	DS11.6
62	ECAT	Ensure systems security	Security testing, surveillance and monitoring	DS5.5
63	IAKM	Ensure systems security	Cryptographic key management	DS5.8
64	CODB	Manage data	Backup and restoration	DS11.5
65	CODP	Ensure continuous service	IT continuity plans	DS4.2
66	COPS	Manage the physical environment	Protection against environmental factors	DS12.4
67	DCAS	Procure IT resources	Supplier selection	AI5.3
68	ECLP	Ensure systems security	User account management	DS5.4
69	ECRR	Ensure systems security	Security testing, surveillance and monitoring	DS5.5
70	ECW M	Ensure systems security	Protection of security technology	DS5.7

#	ICG	COBIT Process Name	COBIT Control Objective Name	COBIT Control Objective
71	PRNK	Ensure systems security	User account management	DS5.4
72	COBR	Manage data	Security requirements for data management	DS11.6
73	COSW	Ensure continuous service	Offsite backup storage	DS4.9
74	COTR	Ensure continuous service	IT services recovery and resumption	DS4.8
75	DCAR	Ensure systems security	IT security plan	DS5.2
76	DCBP	Ensure systems security	User account management	DS5.4
77	DCCT	Manage changes	Impact assessment, prioritisation and authorisation	AI6.2
78	DCDS	Manage third-party services	Supplier risk management	DS2.3
79	DCFA	Define the information architecture	Enterprise information architecture model	PO2.1
80	DCHW	Manage the configuration	Identification and maintenance of configuration items	DS9.2
81	DCID	Ensure systems security	Network security	DS5.10
82	DCII	Manage changes	Impact assessment, prioritisation and authorisation	AI6.2
83	DCIT	Define and manage service levels	Service level agreements	DS1.3
84	DCMC	Ensure systems security	Malicious software prevention, detection and correction	DS5.9
85	DCNR	Ensure systems security	Cryptographic key management	DS5.8
86	DCPD	Procure IT resources	Supplier selection	AI5.3
87	DCPP	Ensure systems security	Network security	DS5.10
88	DCPR	Manage the configuration	(The ICG covers most of the process)	DS9
89	DCSD	Ensure systems security	IT security plan	DS5.2
90	DCSL	Manage data	Media library management system	DS11.3
91	DCSQ	Acquire and maintain application software	Software quality assurance	AI2.8
92	DCSW	Manage the configuration	Identification and maintenance of configuration items	DS9.2
93	EBCR	Ensure systems security	Network security	DS5.10
94	EBVC	Ensure systems security	Network security	DS5.10
95	ECIM	Ensure systems security	Network security	DS5.10
96	ECPA	Ensure systems security	User account management	DS5.4
97	ECRG	Ensure systems security	Security testing, surveillance and monitoring	DS5.5
98	ECSC	Acquire and maintain application software	Configuration and implementation of acquired application software	AI2.5

#	ICG	COBIT Process Name	COBIT Control Objective Name	COBIT Control Objective
99	ECTP	Manage data	Security Requirements for data management	DS11.6
100	ECVI	Ensure systems security	Network security	DS5.10
101	ECVP	Ensure systems security	Malicious software prevention, detection and correction	DS5.9
102	ECWN	Ensure systems security	Network security	DS5.10
103	PEFI	Manage the physical environment	Protection against environmental factors	DS12.4
104	PEMS	Manage the physical environment	Protection against environmental factors	DS12.4
105	PESL	Ensure systems security	User account management	DS5.4
106	PETN	Educate and train users	Delivery of training and education	DS7.2
107	PEVR	Manage the physical environment	Protection against environmental factors	DS12.4
108	PRRB	Ensure systems security	IT security plan	DS5.2
109	VIVM	Ensure systems security	IT security plan	DS5.2

The partition table, sorted on Coverage, is shown below.

Table 44 Partition Table, Sorted on Coverage

#	ICG	Signature	Type	CIA	Span	Impact	Family	Class	Coverage
60	DCSS	2212--	2	I	2	A	SC-24	T	AI2.4
98	ECSC	111---	3	A	1	A	CM-6	O	AI2.5
91	DCSQ	111---	3	I	1	C	SA-11	M	AI2.8
67	DCAS	---111	3	C	1	A	SA-4	M	AI5.3
86	DCPD	111---	3	A	1	C	SA-6	M	AI5.3
77	DCCT	111---	3	A	1	C	SA-11	M	AI6.2
82	DCII	111---	3	I	1	C	CM-4	O	AI6.2
37	PRMP	---211	2	C	2	A	MA-5	O	DS1.3
43	COSP	211---	2	A	2	D	MA-6	O	DS1.3
47	COMS	221---	2	A	2	D	MA-6	O	DS1.3
83	DCIT	111---	3	I	1	A	SA-9	M	DS1.3
27	PESS	---11-	1	C	1	A	MP-4	O	DS11.2
52	ECSD	221---	2	I	2	B	CM-5	O	DS11.3
90	DCSL	111---	3	I	1	C	CM-5	O	DS11.3
13	PEDD	---1--	1	C	1	A	MP-6	O	DS11.4
35	ECTB	11-1--	1	I	1	C	AU-9	T	DS11.5
64	CODB	321---	2	A	3	D	CP-9	O	DS11.5
2	ECCR	---2+31-	0	C	2	Z	SC-28	T	DS11.6
19	ECML	---11-	1	C	1	A	MP-3	O	DS11.6
20	ECRC	---11-	1	C	1	C	SC-4	T	DS11.6
24	PEDI	---11-	1	C	1	A	PE-5	O	DS11.6

#	ICG	Signature	Type	CIA	Span	Impact	Family	Class	Coverage
26	PESP	---11-	1	C	1	C	PL-4	M	DS11.6
30	DCPA	11----	1	I	1	E	SC-2	T	DS11.6
33	ECDC	11----	1	I	1	C	CP-10	O	DS11.6
61	ECCD	2212--	2	I	2	B	AC-3	T	DS11.6
72	COBR	111---	3	A	1	A	CP-9	O	DS11.6
99	ECTP	111---	3	I	1	C	AU-9	T	DS11.6
25	PEPS	---11-	1	C	1	E	PE-3	O	DS12.2
6	PECF	---21-	0	C	2	A	PE-2	O	DS12.3
8	PEPF	---21-	0	C	2	A	PE-3	O	DS12.3
28	PEVC	---11-	1	C	1	A	PE-7+8	O	DS12.3
55	PEEL	221---	2	A	2	D	PE-12	O	DS12.4
56	PEFD	221---	2	A	2	A	PE-13	O	DS12.4
57	PEFS	221---	2	A	2	B	PE-13	O	DS12.4
58	PEHC	221---	2	A	2	C	PE-14	O	DS12.4
59	PETC	221---	2	A	2	D	PE-14	O	DS12.4
66	COPS	321---	2	A	3	D	PE-11	O	DS12.4
103	PEFI	111---	3	A	1	C	PE-13	O	DS12.4
104	PEMS	111---	3	A	1	A	PE-10	O	DS12.4
107	PEVR	111---	3	A	1	A	PE-9	O	DS12.4
78	DCDS	111---	3	I	1	C	SA-9	M	DS2.3
41	COEB	211---	2	A	2	B	PE-17	O	DS4.2
45	COAS	221---	2	A	2	B	CP-7	O	DS4.2
46	COEF	221---	2	A	2	D	CP-2	O	DS4.2
65	CODP	321---	2	A	3	D	CP-2	O	DS4.2
42	COED	211---	2	A	2	D	CP-4	O	DS4.5
74	COTR	111---	3	A	1	A	CP-10	O	DS4.8
73	COSW	111---	3	A	1	A	CP-6	O	DS4.9
10	EBPW	----11	1	C	1	A	SC-7	T	DS5.10
14	EBRP	---11-	1	C	1	A	AC-17	T	DS5.10
15	EBRU	---11-	1	C	1	A	AC-17	T	DS5.10
18	ECIC	---11-	1	C	1	C	AC-4	T	DS5.10
39	EBBD	---321	2	C	3	Z	SC-7	T	DS5.10
50	ECND	221---	2	I	2	D	SC-7	T	DS5.10
81	DCID	111---	3	I	1	A	CA-3	M	DS5.10
87	DCPP	111---	3	A	1	C	CA-3	M	DS5.10
93	EBCR	111---	3	A	1	C	AC-4	T	DS5.10
94	EBVC	111---	3	A	1	C	SI-4	O	DS5.10
95	ECIM	111---	3	I	1	C	AC-4	T	DS5.10
100	ECVI	111---	3	A	1	C	SC-19	T	DS5.10
102	ECWN	111---	3	A	1	A	AC-18	T	DS5.10
1	ECNK	---1+21-	0	C	2	C	SC-9	T	DS5.11
3	ECCT	---21-	0	C	2	B	SC-9	T	DS5.11
7	PECS	---21-	0	C	2	A	MP-6	O	DS5.11
53	ECTM	221---	2	I	2	C	SC-8	T	DS5.11

#	ICG	Signature	Type	CIA	Span	Impact	Family	Class	Coverage
38	DCSR	---321	2	C	3	A	SA-14	M	DS5.2
75	DCAR	111---	3	A	1	C	PL-2	M	DS5.2
89	DCSD	111---	3	A	1	A	PL-2	M	DS5.2
108	PRRB	111---	3	A	1	A	PL-4	M	DS5.2
109	VIVM	111---	3	A	1	C	RA-5	M	DS5.2
16	ECAD	---11-	1	C	1	C	AC-3	T	DS5.3
4	ECLO	---21-	0	C	2	C	AC-7	T	DS5.4
5	IAIA	---21-	0	C	2	A	IA-5	T	DS5.4
9	PRAS	---21-	0	C	2	A	PS-3	O	DS5.4
17	ECAN	---11-	1	C	1	A	AC-3	T	DS5.4
22	IAAC	---11-	1	C	1	A	AC-2	T	DS5.4
23	IAGA	---11-	1	C	1	C	IA-2	T	DS5.4
51	ECPC	221---	2	I	2	C	AC-2	T	DS5.4
68	ECLP	---111	3	C	1	A	AC-6	T	DS5.4
71	PRNK	---111	3	C	1	A	PS-3	O	DS5.4
76	DCBP	111---	3	I	1	C	IA-5	T	DS5.4
96	ECPA	111---	3	I	1	A	AC-2	T	DS5.4
105	PESL	111---	3	I	1	C	AC-11	T	DS5.4
12	ECLC	---1--	1	C	1	E	AU-3	T	DS5.5
21	ECTC	---11-	1	C	1	A	PE-19	O	DS5.5
40	ECAR	---321	2	ICC	3	Z	AU-3	T	DS5.5
62	ECAT	221211	2	I	2	D	AU-6	T	DS5.5
69	ECRR	---111	3	I	1	C	AU-11	T	DS5.5
97	ECRG	111---	3	I	1	E	AU-7	T	DS5.5
32	DCSP	11----	1	I	1	C	SC-3	T	DS5.7
70	ECWM	---111	3	C	1	E	AC-8	T	DS5.7
11	ECCM	---1--	1	C	1	A	SC-12	T	DS5.8
54	IATS	221---	2	I	2	C	IA-5	T	DS5.8
63	IAKM	2213--	2	I	3	C	SC-12	T	DS5.8
85	DCNR	111---	3	I	1	C	AU-10	T	DS5.8
34	ECID	11----	1	I	1	C	SI-4	O	DS5.9
84	DCMC	111---	3	I	1	C	SC-18	T	DS5.9
101	ECVP	111---	3	A	1	A	SI-3	O	DS5.9
29	PRTN	---11-	1	I	1	A	AT-3	O	DS7.2
106	PETN	111---	3	A	1	E	AT-3	O	DS7.2
44	VIIR	211---	2	A	2	B	IR-8	O	DS8
48	DCCB	221---	2	I	2	D	CM-3	O	DS9
88	DCPR	111---	3	I	1	A	CM-9	O	DS9
49	DCCS	221---	2	I	2	A	CM-6	O	DS9.1
80	DCHW	111---	3	A	1	A	CM-8	O	DS9.2
92	DCSW	111---	3	A	1	A	CM-8	O	DS9.2
36	ECMT	---211	2	C	2	D	CA-7	M	ME2.4
79	DCFA	111---	3	I	1	C	PL-2	M	PO2.1
31	DCPB	11----	1	A	1	A	SA-2	M	PO5.1

4 ANALYSIS OF SUBJECT AREAS

This section analyzes the subject areas via the partitions presented in the previous sections. For example, this analysis shows that the ICGs in the EC subject area are of no particular type, CIA, impact, family, or coverage; however, these ICGs are usually in the Technical Class and often are Span 1.

The approach involves two steps. In the first step the correspondence between a subject area and a partition is measured on the following basis:

- If 100% or between 75% and 99% or between 51% and 74% of the subject area ICGs are in any one partition subset of the partition, then we say that the subject area has a "Grade A" or "Grade B" or "Grade C", respectively, correspondence with that partition.
- Otherwise (i.e., no partition subset of the partition has more than 50% of the subject area ICGs) we say that the subject area does not have a correspondence with the partition.

The next table summarizes the previous paragraph by showing (1) the name and percentage range for the three correspondence grades and (2) the range of the number of ICGs in each subject area (where the subject areas are listed from left-to-right in descending order of the number of ICGs in the subject area) that would need to be in one partition subset in order for there to be a correspondence.

For example, if 26 ICGs in subject area EC are in the same partition subset of a given partition, then EC has Grade B correspondence with that partition but if 26 ICGs in subject area DC are in the same partition subset of a given partition, then DC has a Grade A correspondence with that partition. Note that we do not allow subject area VI, because of its small size, to have Grade B or Grade C correspondence but only Grade A.

Table 45 Correspondence Grade Ranges

Grade		Subject Areas							
Name	**Range**	**EC**	**DC**	**PE**	**CO**	**EB**	**IA**	**PR**	**VI**
A	100%	34	26	19	12	6	5	5	2
B	75..99%	25..33	20..25	14..18	9..11	5	4	4	
C	51..74%	18..24	14..19	10..13	7, 8	4	3	3	

In order to familiarize the reader with the tables that follow, an illustrative table is presented next that shows subject area correspondence for a fictitious partition, Partition X, with three fictitious partition subsets—Partition Subset 1, Partition Subset 2, and Partition Subset 3—and with data for the first four subject areas only:

- Subject area EC is shown with Grade A correspondence with Partition Subset 1;
- Subject area DC is shown with Grade B correspondence with Partition Subset 2;
- Subject area PE is shown with Grade C correspondence with Partition Subset 3; and
- Subject area CO is shown with no correspondence.

The cells showing the Grades A, B, and C correspondences are colored red, yellow, and green, respectively.

Table 46 Illustration: Correspondence with Partition X

Partition X	Subject Areas								
	EC	DC	PE	CO	EB	IA	PR	VI	TOTAL
Partition Subset 1	34		11	2					
Partition Subset 2		23	5	6					
Partition Subset 3		3	3	4					
TOTAL	34	26	19	12	6	5	5	2	109

Grade	A	B	C						

The second step in this approach is to gather the correspondence measurements for each of the subject areas for each of the partitions and present those measurements in a table, from which a characterization for each subject area can be made.

The first step is shown below, followed by the second step.

4.1 First Step: Subject Area Correspondence

The correspondence between the subject areas and each partition is considered in turn, starting with the type partition and finishing with the coverage partition.

4.1.1 Type

Subject area CO has Grade B correspondence with Type 2 and DC has Grade C with Type 3, as shown in the next table.

Table 47 Correspondence with Type

Type	Subject Areas								
	EC	DC	PE	CO	EB	IA	PR	VI	TOTAL
0	4		3			1	1		9
1	11	3	6		3	2	1		26
2	8	4	5	9	1	2	1	1	31
3	11	19	5	3	2		2	1	43
TOTAL	34	26	19	12	6	5	5	2	109

Grade		C		B					

4.1.2 CIA

Subject areas CO and VI have Grade A correspondence with Availability. DC has Grade B correspondence with Integrity. And EB, IA, and PR have Grade C correspondence with Confidentiality, as shown in the next table.

Table 48 Correspondence with CIA

Type	Subject Areas								
	EC	DC	PE	CO	EB	IA	PR	VI	TOTAL
Confidentiality	16	2	9		4	3	3		37
Integrity	14	16	1			2	1		34
Availability	4	8	9	12	2		1	2	38
TOTAL	34	26	19	12	6	5	5	2	109

Grade		B		A	C	C	C	A	

4.1.3 Span

Subject areas DC and EB have Grade B correspondence with Span 1 and EC, PE, and PR have Grade C correspondence also with Span 1, as shown in the next table.

Table 49 Correspondence with Span

Span	Subject Areas								
	EC	DC	PE	CO	EB	IA	PR	VI	TOTAL
1	22	22	11	3	5	2	3	1	69
2	11	3	8	6		2	2	1	33
3	1	1		3	1	1			7
TOTAL	34	26	19	12	6	5	5	2	109

Grade	C	B	C		B		C		

4.1.4 Impact

Subject area PR has Grade A correspondence with Priority A and PE, CO, and IA have Grade C with Priorities A, D, and C, respectively, as shown in the next table.

Table 50 Correspondence with Impact

Impact Priority	Subject Areas								
	EC	DC	PE	CO	EB	IA	PR	VI	TOTAL
A	9	11	10	3	3	2	5		43
B	3		1	2				1	7
C	14	13	4		2	3		1	37
D	3	1	2	7					13
E	3	1	2						6
Z	2				1				3
TOTAL	34	26	19	12	6	5	5	2	109

Grade			C	C		C	A		

4.1.5 Family

Subject areas PE, CO, and IA have Grade C correspondence with Families PE, CP, and IA, respectively, as shown in the next table.

Table 51 Correspondence with Family

Family	Subject Areas								
	EC	DC	PE	CO	EB	IA	PR	VI	TOTAL
AC	11		1		3	1			16
AT			1				1		2
AU	7	1							8
CA	1	2							3
CM	2	7							9
CP	1			8					9
IA		1				3			4
IR								1	1
MA				2			1		3
MP	1		3						4
PE	1		13	2					16
PL		2	1				1		4
PS							2		2
RA								1	1
SA		8							8
SC	8	4			2	1			15
SI	2				1				3
PM		1							1
TOTAL	34	26	19	12	6	5	5	2	109
Grade			C	C		C			

There are 18 families but only eight subject areas, diluting the correspondence. The correspondence is more evident if we pair up the families, leaving us almost the same number of combined families as subject areas. Accordingly, the paired families, where similarity of purpose was used to choose the pairs, are shown in the next table.

Table 52 Combined Families

Combined Identifier	Families	Class	Combined Controls	Combined Matching ICGs from 8500.2
AC+IA	Access Control + Identification and Authentication	Technical	19 + 8 = 27	16 + 4 = 20
AT+PS	Awareness and Training + Personnel Security	Operational	5 + 8 = 13	2 +2 = 4
AU+SC	Audit and Accountability + System and	Technical	14 + 34 = 48	8 + 15 = 23

Combined Identifier	Families	Class	Combined Controls	Combined Matching ICGs from 8500.2
	Communications Protection			
CA+RA	Security Assessment and Authorization + Risk Assessment	Management	6 + 4 = 10	3 +1 = 4
CM+SI	Configuration Management + System and Information Integrity	Operational	9 + 13 = 22	9 + 3 = 12
CP+IR	Contingency Planning + Incident Response	Operational	9 + 8 = 17	9 + 1 = 10
MA+SA	Maintenance + System and Services Acquisition	Operational + Management	6 + 14 = 20	3 + 8 = 11
MP+PE	Media Protection + Physical and Environmental Protection	Operational	6 + 19 = 25	4 + 16 = 20
PL+PM	Planning + Program Management	Management	5 + 11 = 16	4 + 1 = 5
TOTAL	9		198	109

Using the combined families, subject areas PE and IA now have Grade B correspondence with MP+PE and AC+IA, respectively, and CO and PR have Grade C correspondence with CP+IR and AT+PS, respectively, as shown in the next table.

Table 53 Correspondence with Family (Combined)

Family	Subject Areas								
	EC	DC	PE	CO	EB	IA	PR	VI	TOTAL
AC+IA	11	1	1		3	4			20
AT+PS			1				3		4
AU+SC	15	5			2	1			23
CA+RA	1	2						1	4
CM+SI	4	7			1				12
CP+IR	1			8				1	10
MA+SA		8		2			1		11
MP+PE	2		16	2					20
PL+PM		3	1				1		5
TOTAL	34	26	19	12	6	5	5	2	109

Grade			B	C		B	C		

4.1.6 Class

Subject areas CO and IA have Grade A correspondence with the Operational and Technical classes, respectively, and EC, PE, EB, and PR have Grade B correspondence with the Technical, Operational, Technical, and Operational classes, respectively, as shown in the next table.

Table 54 Correspondence with Class

Span	Subject Areas								
	EC	DC	PE	CO	EB	IA	PR	VI	TOTAL
Management	1	13	1				1	1	17
Operational	7	7	17	12	1		4	1	49
Technical	26	6	1		5	5			43
TOTAL	34	26	19	12	6	5	5	2	109

Grade	B		B	A	B	A	B		

4.1.7 Coverage

Correspondence with the subject areas requires arranging COBIT's sets. Accordingly we construct the following sets:

- Set W consists of the ICGs that are not in Domain DS.
- Set X consists of the ICGs in DS but not in DS5, DS11, or DS12.
- Set 11 consists of the ICGs in DS11.
- Set 12 consists of the ICGs in DS12.
- Set 5.Y consists of the ICGs in DS5 that are not in DS5.4, DS5.5, or DS5.10.
- Set 5.4 consists of the ICGs in DS5.4.
- Set 5.5 consists of the ICGs in DS5.5.
- Set 5.10 consists of the ICGs in DS5.10.

The next figure shows the relationship between these sets graphically.

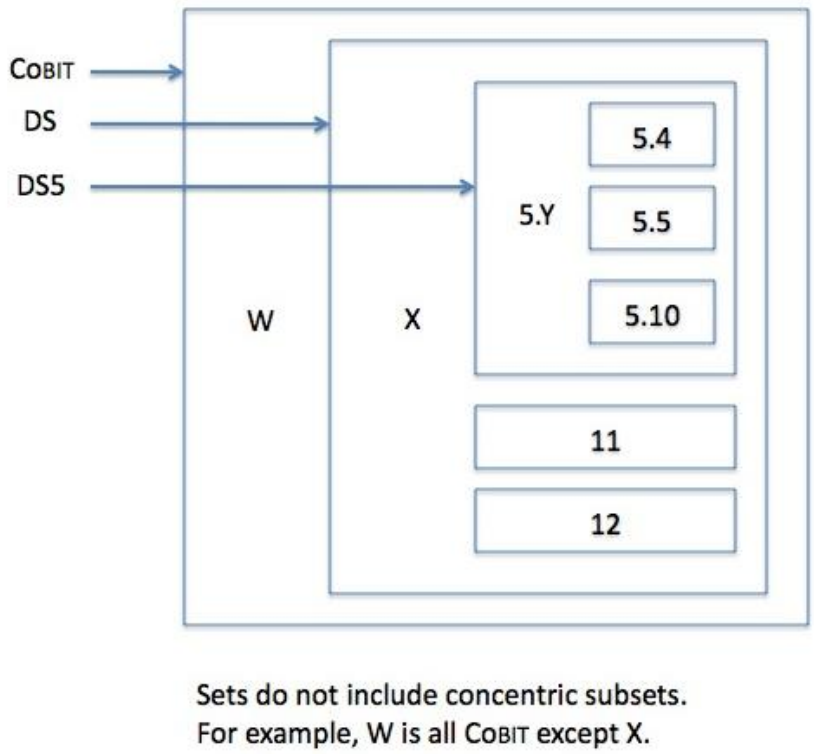

Figure 2 Coverage Correspondence Sets

Using the set arrangement shown above, subject area EB has Grade A correspondence with 5.10, CO has Grade B correspondence with X, and PE and IA have Grade C correspondence with Sets 12, and 5.4 respectively, as shown in the next table.

Table 55 Correspondence with Coverage

Coverage	Subject Areas								
	EC	DC	PE	CO	EB	IA	PR	VI	TOTAL
W	2	8							10
X	1	7	1	9			2	1	21
11	7	2	4	2					15
12			11	1					12
5.Y	6	6	1			2	1	1	17
5.4	5	1	2			3	2		13
5.5	8								8
5.10	5	2			6				13
TOTAL	34	26	19	12	6	5	5	2	109

Grade			C	B	A	C			

4.2 Second Step: Subject Area Correspondence

This section combines the correspondence measurements presented in the previous section and then, from those combined measurements, characterizes the subject areas.

The next table shows the combined correspondence measurements, coloring the table according to the correspondence, as explained in the previous section, and specifying the partition subset (see the key below). In order to compare the results we arbitrarily assign 1, 2, and 3 points for a Grade C, B, and A correspondence, respectively, for a maximum of 21 points, and show a sum in the last row in the table.

Table 56 Correspondence Summary

Partition	Subject Area							
	EC	DC	PE	CO	EB	IA	PR	VI
Type		3		2				
CIA		I		A	C	C	C	A
Span	1	1	1		1		1	
Impact			A	D		C	A	
Family (Combined)			MP+PE	CP+IR		AC+IA	AT+PS	
Class	T		O	O	T	T	O	
Coverage			12	X	5.10	5.4		
POINTS	3	5	7	12	8	8	8	3

Key:

- Grade:
  - Grade A
  - Grade B
  - Grade C
- Type:
  - 2 = universal & varying robustness
  - 3 = universal & constant robustness
- CIA:
  - C = Confidentiality
  - I = Integrity
  - A = Availability
- Impact:
  - A = high
  - C = medium
  - D = between medium & low
- Family (Combined):
  - AC+IA = Access Control + Identification and Authentication
  - AT+PS = Awareness and Training + Personnel Security
  - CP+IR = Contingency Planning + Incident Response
  - MP+PE = Media Protection + Physical and Environmental Protection
- Class:

    - O = Operational
    - T = Technical
- Coverage:
    - 12 = Manage the physical environment
    - X = Deliver and Support, excluding DS5, 11, and 12
    - 5.10 = Network security
    - 5.4 = User account management

The point totals suggest that the ICGs in CO as a group have a focus and that the ICGs in EC and VI do not, based on the partitions.

The paragraphs below translate the table above into text, using the words "always," "usually," and "often" to distinguish Grades A, B, and C, respectively.

Enclave and Computing Environment (EC):

> The EC ICGs are usually in the Technical Class and are often Span 1.

Security Design & Configuration (DC):

> The DC ICGs usually deal with Integrity, are usually Span 1, and are often Type 3.

Physical and Environmental (PE):

> The PE ICGs are usually in the MP & PE families and are usually in the Operational Class. They are often Span 1, often have high Impact, and often deal with managing the physical environment.

Continuity (CO):

> The CO ICGs always deal with Availability and are always in the Operational Class. They are usually Type 2 and are usually in the Deliver and Support Domain. They are often of between medium and low Impact and are often in the CP & IR families.

Enclave Boundary Defense (EB):

> The EB ICGs always deal with network security. They are usually Span 1 and are usually in the Technical Class. They often deal with Confidentiality.

Identification and Authentication (IA):

> The IA ICGs are always in the Technical Class. They are often in the AC & IA families. They often deal with Confidentiality, often have medium Impact, and often deal with user account management.

Personnel (PR):

The PR ICGs are always high Impact. They are usually in the Operational Class. They often deal with Confidentiality, are often Span 1, and are often in the AT & PS families.

Vulnerability and Incident Management (VI):

The VI ICGs always deal with Availability.

5 ANALYSIS OF BASELINE IA LEVELS

This section analyzes the baseline IA levels. In particular, this section determines the relative amount of work required to comply with the IACNs associated with different baseline IA levels.[38] That is, this section computes the "jump" (or work differential) in compliance effort from one of the nine baseline IA levels to another. We would like to know, for example, which of the following requires the smaller increase in work, when starting from a MAC II Sensitive system:

- moving to a MAC I Sensitive system, or
- moving to a MAC II Classified system?

This section uses the name "community" for a group of baseline IA levels such that the differential of a move between baseline IA levels within the group is smaller than the differential of a move to a baseline IA level outside the group.

A change in baseline IA level can change the number of ICGs and/or the robustness level of the existing ICGs. This change we refer to as a "category differential." Both parameters monotonically increase when measuring the changes from MAC III to MAC II to MAC I and from Public to Sensitive to Classified, just as we expect. (The only exception to this rule is ICG EPBW. This ICG, with signature ----11, is *removed* when moving from Sensitive to Classified.) To simplify presentation, we assign the MAC III Public baseline IA level to be the reference point and consider moves

- from MAC III to MAC II to MAC I and
- from Public to Sensitive to Classified

and do not consider moves in the opposite direction The work for moves in the opposite direction are in all cases of the same magnitude but are negative instead of positive.

Analysis proceeds in two steps. In the first step, two sets of communities are identified, one based on the *number of ICGs* that change as we move between MACs and confidentiality levels and the second based on the *increase in robustness levels* as we move between MACs and confidentiality levels. In the second step the two sets of communities identified in the first step are combined to provide a single community.

5.1 First Step: Identify ICG and Robustness Communities

This section identifies the ICG and robustness communities, independently of each other. We first tabulate what we will refer to as "basic differentials," which are the number of ICGs added and robustness level increases when moving not between baseline IA levels but rather between

---

[38] Recall that 8500.2 partitions systems into nine "baseline IA levels," such as MAC I Classified, MAC II Sensitive, and so on.

MACs and confidentiality levels. The eight ICGs with signatures that do not fit the patterns followed by the other ICGs, as described in the section on type above, require the following ad hoc rules.

We count an increase in robustness of one, not zero, for ECNK, with signature ---1+21-, when moving from Sensitive to Classified.

We count an increase in robustness of only one, not two, for ECCR, with signature ---2+31-, when moving from Sensitive to Classified.

We do not subtract an ICG for EPBW, with signature ----11, when moving from Sensitive to Classified. (However, the subtraction is noted with a "-x" in the Additions table below.)

We add an ICG for ECTB, with signature 11-1--, when moving from MAC III to MAC II and when moving from Sensitive to Classified (see next table).

Table 57 Robustness Levels for ICG ECTB (Signature 11-1--)

	MAC I	MAC II	MAC III
Classified	1	1	1
Sensitive	1	1	-
Public	1	1	-

We count an increase in robustness for ICGs DCSS, ECCD, and ECAT, all with signatures 2212– (ECAT's signature is 221211 but this is equivalent, as shown above, to 2212--), and for ICG IAKM, with signature 2213--, when moving from MAC III to MAC II and when moving from Sensitive to Classified (see next table).

Table 58 Robustness Levels for ICG DCSS (Signature 2212--)

	MAC I	MAC II	MAC III
Classified	2	2	2
Sensitive	2	2	1
Public	2	2	1

The contribution to the basic differentials of the Type 0, 1, and 2 ICGs is shown in the next table.[39]

[39] When we move between baseline IA levels, ICGs of Type 0 and 1 can change the number of ICGs, and ICGs of Type 0 and 2 can change the robustness. ICGs of Type 3 do not change either the number of ICGs or the robustness and are thus not relevant to this discussion. ICG EBPW, like a Type 3 ICG, does not change the number of ICGs or robustness, given the ad hoc rule shown above, but EBPW is included in the table for completeness.

Table 59 ICG and Robustness Additions[40]

#	ICG	Signature	ICG Added				Robustness Added			
			I←II	II←III	C←S	S←P	I←II	II←III	C←S	S←P
1	ECNK	---1+21-				x			x	
2	ECCR	---2+31-				x			x	
3	ECCT	---21-				x			x	
4	ECLO	---21-				x			x	
5	IAIA	---21-				x			x	
6	PECF	---21-				x			x	
7	PECS	---21-				x			x	
8	PEPF	---21-				x			x	
9	PRAS	---21-				x			x	
10	EBPW	----11			-x[41]					
11	ECCM	---1--			x					
12	ECLC	---1--			x					
13	PEDD	---1--			x					
14	EBRP	---11-				x				
15	EBRU	---11-				x				
16	ECAD	---11-				x				
17	ECAN	---11-				x				
18	ECIC	---11-				x				
19	ECML	---11-				x				
20	ECRC	---11-				x				
21	ECTC	---11-				x				
22	IAAC	---11-				x				
23	IAGA	---11-				x				
24	PEDI	---11-				x				
25	PEPS	---11-				x				
26	PESP	---11-				x				
27	PESS	---11-				x				
28	PEVC	---11-				x				
29	PRTN	---11-				x				
30	DCPA	11----		x						
31	DCPB	11----		x						
32	DCSP	11----		x						
33	ECDC	11----		x						
34	ECID	11----		x						

[40] Column header explanations: "I←**II**" denotes "MAC II to MAC I" (similarly "**II←III**"), "**C←S**" denotes "Sensitive to Classified," and "**S←P**" denotes "Public to Sensitive." This right-to-left notation conflicts with the English left-to-right explanation but it matches the arrangement in the signatures, which follow the Attachment sequence, making the table easier to read.

[41]This notation is intended to remind the reader that EBPW, alone among the IACs, is subtracted when moving from Sensitive to Classified. (No IACs are dropped when moving from Public to Sensitive.)

#	ICG	Signature	ICG Added				Robustness Added			
			I←II	II←III	C←S	S←P	I←II	II←III	C←S	S←P
35	ECTB	11-1--		x	x					
36	ECMT	---211							x	
37	PRMP	---211							x	
38	DCSR	---321							x	x
39	EBBD	---321							x	x
40	ECAR	---321							x	x
41	COEB	211---					x			
42	COED	211---					x			
43	COSP	211---					x			
44	VIIR	211---					x			
45	COAS	221---						x		
46	COEF	221---						x		
47	COMS	221---						x		
48	DCCB	221---						x		
49	DCCS	221---						x		
50	ECND	221---						x		
51	ECPC	221---						x		
52	ECSD	221---						x		
53	ECTM	221---						x		
54	IATS	221---						x		
55	PEEL	221---						x		
56	PEFD	221---						x		
57	PEFS	221---						x		
58	PEHC	221---						x		
59	PETC	221---						x		
60	DCSS	2212--						x	x	
61	ECCD	2212--						x	x	
62	ECAT	221211						x	x	
63	IAKM	2213--						x	x	
64	CODB	321---					x	x		
65	CODP	321---					x	x		
66	COPS	321---					x	x		

The basic differentials are shown in the next table.

Table 60 Basic Differentials

From	To	ICGs Added	Increase in Robustness
MAC III	**MAC II**	6	22
MAC II	**MAC I**	0	7
Public	**Sensitive**	25	3
Sensitive	**Classified**	4	18

The table above shows that the move from Public to Sensitive adds the most ICGs (by a factor of over 4) and that the move from MAC III to MAC II increases robustness the most.

The next table shows the ICG category differentials, based on the basic differentials shown above.

Table 61 ICG Category Differentials[42]

	MAC I	MAC II	MAC III
Classified	35	35	29
Sensitive	31	31	25
Public	6	6	0

The next figure displays the previous table in graphical form, facilitating the identification of ICG communities.

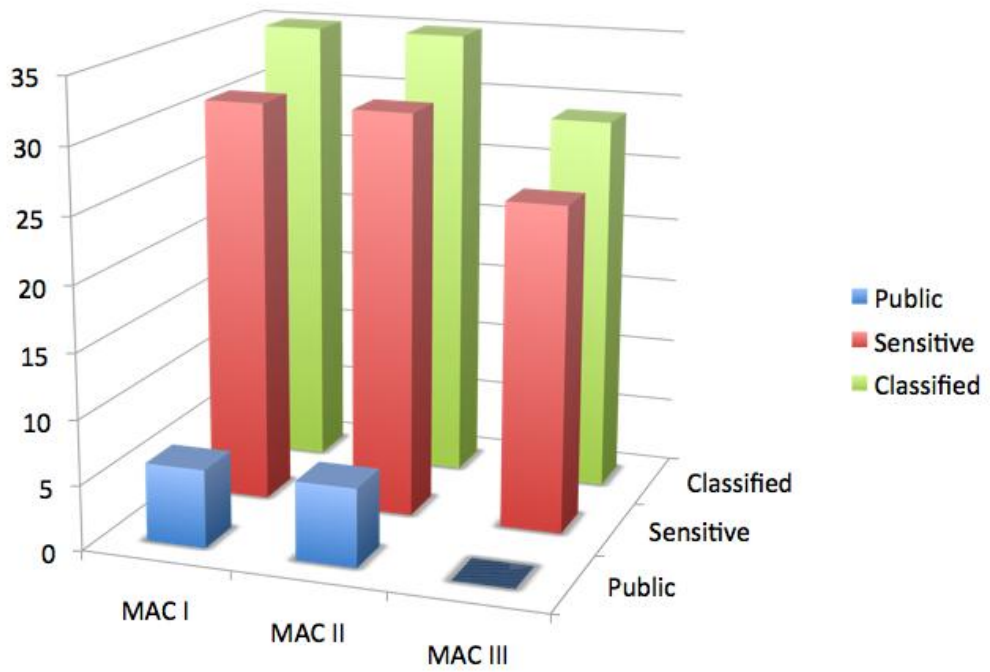

Figure 3 ICGs Category Differentials

For ICG category differentials, the table and chart above suggest five communities, where the communities here and elsewhere in this section are established intuitively:

1. MAC III, Public
2. MAC I & II Public

[42] To read this table, start with the Public MAC III cell, then note, for example, that moving to the Sensitive MAC III cell adds 25 ICGs and moving to the Public MAC II cell adds 6 ICGs.

3. MAC III Sensitive
4. MAC I & II Sensitive and MAC III Classified
5. MAC I & II Classified

The next table shows the five communities.

Table 62 ICG Communities

	MAC I	MAC II	MAC III
Classified	5	5	4
Sensitive	4	4	3
Public	2	2	1

For robustness differentials the next table and the subsequent chart identify the basis for robustness communities.

Table 63 Robustness Category Differentials

	MAC I	MAC II	MAC III
Classified	50	43	21
Sensitive	32	25	3
Public	29	22	0

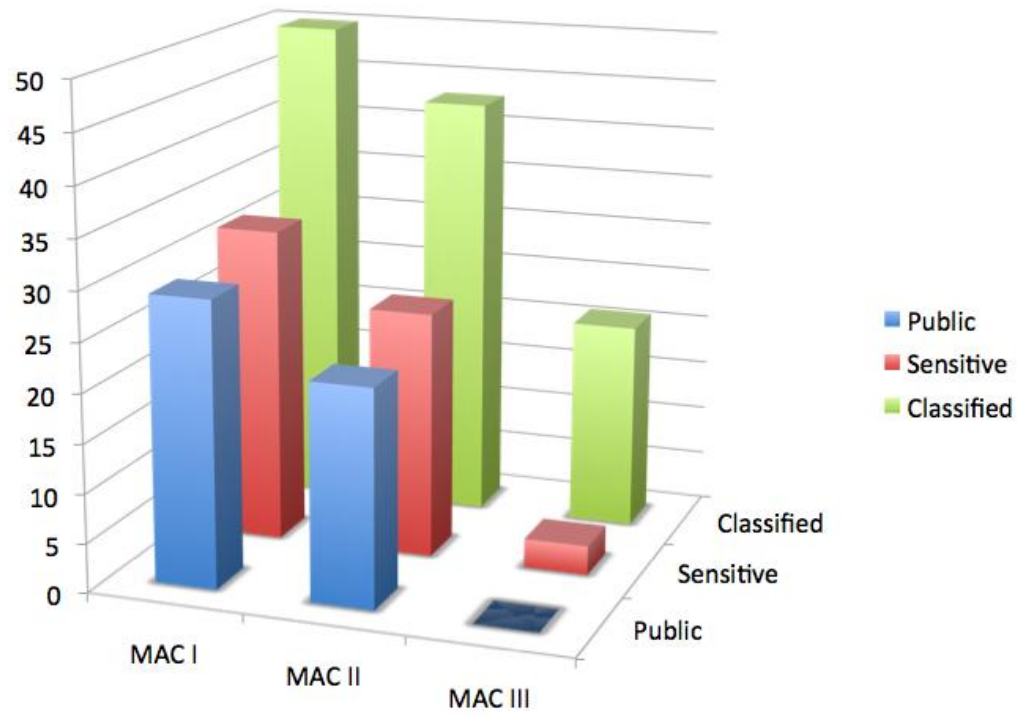

Figure 4 Robustness Category Differentials

For robustness differentials, the table and chart above suggest four communities:

1. MAC III Sensitive & Public,
2. MAC III Classified and MAC II Sensitive & Public,
3. MAC I Sensitive & Public, and
4. MAC I & II Classified[43].

The next table shows the four communities.

Table 64 Robustness Communities

	MAC I	MAC II	MAC III
Classified	4	4	2
Sensitive	3	2	1
Public	3	2	1

5.2 Second Step: Combine ICG and Robustness Communities

In order to combine the ICG and robustness communities presented in the previous section we need an equation that relates the work increase due to an added ICG and the work increase due to an increase in robustness. Based on informal consideration we make the following assumption:

> Assumption 1: The work increase due to an added ICG is twice the work increase due to an increase in robustness.

The above assumption gives us the needed equation, namely

$$B = 2 * R$$

where

- B denotes the work increase due to an added ICG and
- R denotes the work increase due to an increase in robustness.

The combined, base differentials, using the above equation, are shown in the rightmost column in the next table.

Table 65 Base Differentials (Combined)

From	To	ICGs Added	Increase in Robustness	Combined
MAC III	**MAC II**	6	22	6*2 + 22 = 34
MAC II	**MAC I**	0	7	0*2 + 7 = 7
Public	**Sensitive**	25	3	25*2 + 3 = 53
Sensitive	**Classified**	4	18	4*2 + 18 = 26

[43] An argument could be made that these are two communities, not one.

The next table and chart show the category differentials that form the basis for communities.

Table 66 Category Differentials (Combined)

	MAC I	MAC II	MAC III
Classified	120	113	79
Sensitive	94	87	53
Public	41	34	0

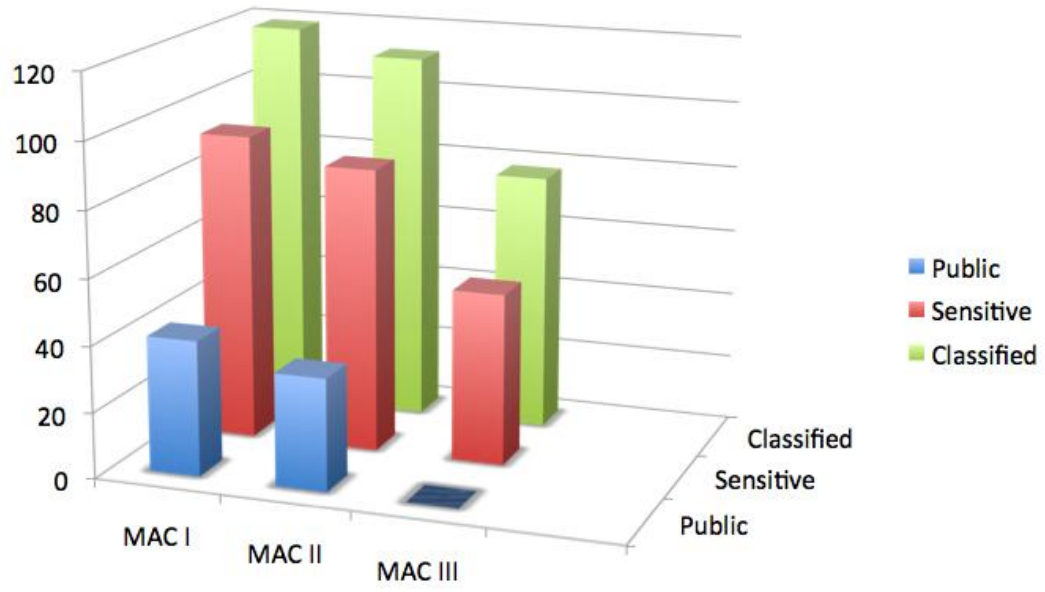

Figure 5 Combined Category Differentials

For category differentials, the table and chart above suggests four communities:

1. MAC III Public,
2. MAC III Sensitive and MAC I & II Public,
3. MAC III Classified and MAC I & II Sensitive, and
4. MAC I & II Classified.

The next table shows the four communities.

Table 67 Combined Communities

	MAC I	MAC II	MAC III

Classified	4	4	3
Sensitive	3	3	2
Public	2	2	1

We are now in a position to answer the question posed at the beginning of this section, namely, from a MAC II Sensitive system, which requires the smaller increase in work:

- Moving to a MAC I Sensitive system, or
- Moving to a MAC II Classified system?

We see that moving from a MAC II Sensitive system to a MAC I Sensitive system has a work differential of 7, and moving from a MAC II Sensitive system to a MAC II Classified system has a work differential of 26, so the former is the easier.

6 SUMMARY

In general, this report partitioned the 8500.2 ICGs based on a number of partitions, namely type, CIA, span, impact, family, class, and coverage. Each partition is a different view of the ICGs and thus provides insight. These partitions were then used to provide insight into the subject area partition given by 8500.2. Finally, community—a partition of the baseline IA levels given by 8500.2—was presented that provides insight into the work differentials between baseline IA levels.

In particular, from this report we learn that the 298 IA Control appearances in DoDI 8500.2 reduce to 109 IA Control Groups (ICGs). Each ICG has a "signature" that indicates in which of the six attachments an instance of an ICG appears and the robustness level of the appearance. There are four types of signatures. Of particular interest are Type 3 ICGs, of which there are 43, which apply to all nine baseline IA levels without variation of robustness level. There are four patterns to the set of signatures and eight of the ICGs do not conform to these patterns. Some of these non-conformities could be eliminated by various editorial changes and others would require more fundamental changes. The signatures in the set of 109 ICGs cover all of the allowable signatures.

The ICGs are slightly more focused on providing availability and confidentiality than on providing integrity, based on the number of ICGs. The attachments have a stated focus but a pattern reveals five ICGs for which there is a mismatch between the ICG and the intent of the attachment in which the ICG appears. (And there is one ICG that is marked for both integrity and confidentiality.)

Only 7 of the 109 ICGs have IA Controls for all three robustness levels. Most of the ICGs (69) have only one robustness level.

There are more ICGs than expected for which it should be a high priority to bring into compliance and there are only a few at the other end of the spectrum. This suggests a dilution of the priority scheme.

Based on a comparison with NIST 800-53 almost half of the ICGs are concerned with

1. Access Control,
2. Physical & Environmental Protection, and
3. System & Communication Protection.

The other half of the ICGs map to each of the "families" in NIST 800-53. So 8500.2 has breadth but it focuses on depth.

There are more ICGs that focus on Operational and Technical issues than focus on Management issues, based again on the number of ICGs. This suggests an emphasis on the former at the expense of the latter.

Based on a comparison with COBIT from the IT Governance Institute, the ICGs are concerned with "Delivery and Support" in general and user account management and network security in particular.

Based on the partitions used as the basis for the analysis of this report, summarized above, the Continuity subject area seems to be the most focused and the Enclave & Computer Environment and Vulnerability & Incident Management subject areas the least focused.

The nine baseline IA levels appear to reduce to four "communities," where community is defined such that the differential in the amount of work required by the set of IA Controls between two baseline IA levels within a community is smaller than the differential of a move to a baseline IA level outside the group. The four communities are as follows:

1. MAC III Public,
2. MAC III Sensitive and MAC I & II Public,
3. MAC III Classified and MAC I & II Sensitive, and
4. MAC I & II Classified.

There are a number of next steps. For example,

- What is the relationship between the partitions? This report examines each partition in isolation, but what do span and family, say, together reveal about the ICGs?
- What are the dependencies between ICGs? Do any ICGs work at cross purposes to other ICGs?
- What is the relationship between the lifecycle and the ICGs? Is there an optimal time in the lifecycle for a given ICG to be implemented?
- Are different implementations of the ICGs possible? How effective are these different implementations? How do the implementation and maintenance costs vary?
- What protection do various ICGs provide against insider attack?
- What ICGs provide protection against the most likely attacks, given attack lists provided by organizations such as SANS?
- How effective are mitigations in reducing the need to implement certain ICGs, again given lists provided by organizations such as SANS?

REFERENCES

1. Control Objectives for Information and Related Technology (COBIT ®) 4.1. (COBIT is available at no cost from www.itgi.org.)
2. Debra S. Herrmann, Complete Guide to Security and Privacy Metrics (2007), Auerbach Publications, Boca Raton, Florida. ISBN 0-8493-5402-1.
3. Department of Defense Instruction, Number 8500.2, SUBJECT: "Information Assurance (IA) Implementation," February 6, 2003, 102 pages.
4. DIACAP: Department of Defense Instruction, Number 8510.01, SUBJECT: "DoD Information Assurance and Accreditation Process (DIACAP)," November 28, 2007, 53 pages.
5. DoD Knowledge Service (https://diacap.iaportal.navy.mil).
6. Federal Information Processing Standards Publication (FIPS) PUB 199, "Standards for Security Categorization of Federal Information and Information Systems," Computer Science Division, Information Technical Laboratory, National Institute of Standards and Technology (NIST), February 2004, 13 pages.
7. Federal Information Processing Standards Publication (FIPS) PUB 200, "Minimum Security Requirements for Federal Information and Information Systems," Computer Science Division, Information Technical Laboratory, National Institute of Standards and Technology (NIST), March 2006, 11 pages.
8. ISACA (www.isaca.org).
9. IT Governance Institute (www.itgi.org).
10. National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations," August 2009, approximately 160 pages.
11. Space and Naval Warfare Systems Command (SPAWAR), "Certification Guide," Version 1.1, May 18, 2001.

7 APPENDIX A: GALLERY OF UNUSUAL ELEMENTS

This report has partitioned the 8500.2 ICGs in various ways. Along the way unusual ICGs have come to light, where "unusual" means that these ICGs have some characteristics shared by only a few other ICGs. This appendix lists some of these unusual ICGs.

ECCR and ECNK are the only ICGs that do not conform to Pattern 0.

EBPW is the only ICG that does not conform to Pattern 1.

DCSS, ECAT, ECCD, ECTB, and IAKM are the only ICGs that do not conform to Pattern 2.

ECAR is the only ICG that is marked for more than one of {Confidentiality, Integrity, Availability}.

CODB, CODP, COPS, DCSR, EBBD, ECAR, and IAKM are the only Span 3 ICGs.

DCPA, ECLC, ECRG, ECWM, PEPS, and PETN are the only Impact Priority E ICGs.

EBBD, ECAR, and ECCR are the only Impact Priority Z ICGs.

ECCM, ECLC, and PEDD are the only ICGs for which there is only one IAC (and they all appear in Attachment 4).

EPBW is the only ICG that is removed when moving along any of the following changes: from MAC III to MAC II to MAC I or from Public to Sensitive to Classified. EPBW is removed when moving from Sensitive to Classified (signature ----11).

IAAC is the only ICG that appears outside of the list of ICGs in its subject area in an attachment (IAC:233 and IAC:270 in Attachments A4 and A5, respectively).

Attachment A4 is the only attachment that has an ICG for which there are two appearances. There are two such ICGs—ECNK and ECCR—and they both appear in Attachment A4.

We could conclude that Attachment 4, that addresses the classified confidentiality level, is the most unusual attachment.

8 APPENDIX B: IACS

This Appendix presents two tables, both with the same layout and content but sorted differently. Both tables show each of the 298 IACs, their IA Control Number (IACN), their IA Control Name, their appearance index, and the page number and attachment in 8500.2 in which they appear. The first table is sorted on appearance index—this is the order in which the IACs appear in 8500.2—and the second table is sorted on attachment within IACN.

Table 68 IACs, Sorted on Appearance Index

IACN	IA Control Name	Appearance Index	Page	Attachment
DCAR-1	Procedural Review	1	54	A1
DCBP-1	Best Security Practices	2	54	A1
DCCB-2	Control Board	3	54	A1
DCCS-2	Configuration Specifications	4	54	A1
DCCT-1	Compliance Testing	5	54	A1
DCDS-1	Dedicated IA Services	6	54	A1
DCFA-1	Functional Architecture for AIS Applications	7	55	A1
DCHW-1	HW Baseline	8	55	A1
DCID-1	Interconnection Documentation	9	55	A1
DCII-1	IA Impact Assessment	10	55	A1
DCIT-1	IA for IT Services	11	55	A1
DCMC-1	Mobile Code	12	56	A1
DCNR-1	Non-repudiation	13	56	A1
DCPA-1	Partitioning the Application	14	56	A1
DCPB-1	IA Program and Budget	15	56	A1
DCPD-1	Public Domain Software Controls	16	57	A1
DCPP-1	Ports, Protocols, and Services	17	57	A1
DCPR-1	CM Process	18	57	A1
DCSD-1	IA Documentation	19	57	A1
DCSL-1	System Library Management Controls	20	57	A1
DCSP-1	Security Support Structure Partitioning	21	58	A1
DCSQ-1	Software Quality	22	58	A1

IACN	IA Control Name	Appearance Index	Page	Attachment
DCSS-2	System State Changes	23	58	A1
DCSW-1	SW Baseline	24	58	A1
IAKM-2	Key Management	25	58	A1
IATS-2	Token and Certificate Standards	26	58	A1
ECAT-2	Audit Trail, Monitoring, Analysis and Reporting	27	58	A1
ECCD-2	Changes to Data	28	58	A1
ECDC-1	Data Change Controls	29	59	A1
ECID-1	Host Based IDS	30	59	A1
ECIM-1	Instant Messaging	31	59	A1
ECND-2	Network Device Controls	32	59	A1
ECPA-1	Privileged Account Control	33	59	A1
ECPC-2	Production Code Change Controls	34	59	A1
ECRG-1	Audit Reduction and Report Generation	35	59	A1
ECSC-1	Security Configuration Compliance	36	59	A1
ECSD-2	Software Development Change Controls	37	60	A1
ECTB-1	Audit Trail Backup	38	60	A1
ECTM-2	Transmission Integrity Controls	39	60	A1
ECTP-1	Audit Trail Protection	40	60	A1
ECVI-1	Voice-over-IP (VoIP) Protection	41	60	A1
ECVP-1	Virus Protection	42	60	A1
ECWN-1	Wireless Computing and Network	43	60	A1
EBCR-1	Connection Rules	44	61	A1
EBVC-1	VPN Controls	45	61	A1
PEEL-2	Emergency Lighting	46	61	A1
PEFD-2	Fire Detection	47	61	A1
PEFI-1	Fire Inspection	48	61	A1
PEFS-2	Fire Suppression	49	61	A1
PEHC-2	Humidity Controls	50	61	A1
PEMS-1	Master Power Switch	51	61	A1
PESL-1	Screen Lock	52	62	A1
PETC-2	Temperature Controls	53	62	A1

IACN	IA Control Name	Appearance Index	Page	Attachment
PETN-1	Environmental Control Training	54	62	A1
PEVR-1	Voltage Regulators	55	62	A1
PRRB-1	Security Rules of Behavior or Acceptable Use Policy	56	62	A1
COAS-2	Alternate Site Designation	57	62	A1
COBR-1	Protection of Backup and Restoration Assets	58	62	A1
CODB-3	Data Backup Procedures	59	62	A1
CODP-3	Disaster and Recovery Planning	60	63	A1
COEB-2	Enclave Boundary Defense	61	63	A1
COED-2	Scheduled Exercises and Drills	62	63	A1
COEF-2	Identification of Essential Functions	63	63	A1
COMS-2	Maintenance Support	64	63	A1
COPS-3	Power Supply	65	63	A1
COSP-2	Spares and Parts	66	63	A1
COSW-1	Backup Copies of Critical SW	67	63	A1
COTR-1	Trusted Recovery	68	63	A1
VIIR-2	Incident Response Planning	69	64	A1
VIVM-1	Vulnerability Management	70	64	A1
DCAR-1	Procedural Review	71	65	A2
DCBP-1	Best Security Practices	72	65	A2
DCCB-2	Control Board	73	65	A2
DCCS-2	Configuration Specifications	74	65	A2
DCCT-1	Compliance Testing	75	65	A2
DCDS-1	Dedicated IA Services	76	65	A2
DCFA-1	Functional Architecture for AIS Applications	77	66	A2
DCHW-1	HW Baseline	78	66	A2
DCID-1	Interconnection Documentation	79	66	A2
DCII-1	IA Impact Assessment	80	66	A2
DCIT-1	IA for IT Services	81	66	A2
DCMC-1	Mobile Code	82	67	A2
DCNR-1	Non-repudiation	83	67	A2
DCPA-1	Partitioning the Application	84	67	A2

IACN	IA Control Name	Appearance Index	Page	Attachment
DCPB-1	IA Program and Budget	85	67	A2
DCPD-1	Public Domain Software Controls	86	68	A2
DCPP-1	Ports, Protocols, and Services	87	68	A2
DCPR-1	CM Process	88	68	A2
DCSD-1	IA Documentation	89	68	A2
DCSL-1	System Library Management Controls	90	69	A2
DCSP-1	Security Support Structure Partitioning	91	69	A2
DCSQ-1	Software Quality	92	69	A2
DCSS-2	System State Changes	93	69	A2
DCSW-1	SW Baseline	94	69	A2
IAKM-2	Key Management	95	69	A2
IATS-2	Token and Certificate Standards	96	69	A2
ECAT-2	Audit Trail, Monitoring, Analysis and Reporting	97	69	A2
ECCD-2	Changes to Data	98	70	A2
ECDC-1	Data Change Controls	99	70	A2
ECID-1	Host Based IDS	100	70	A2
ECIM-1	Instant Messaging	101	70	A2
ECND-2	Network Device Controls	102	70	A2
ECPA-1	Privileged Account Control	103	70	A2
ECPC-2	Production Code Change Controls	104	70	A2
ECRG-1	Audit Reduction and Report Generation	105	70	A2
ECSC-1	Security Configuration Compliance	106	71	A2
ECSD-2	Software Development Change Controls	107	71	A2
ECTB-1	Audit Trail Backup	108	71	A2
ECTM-2	Transmission Integrity Controls	109	71	A2
ECTP-1	Audit Trail Protection	110	71	A2
ECVI-1	Voice-over-IP (VoIP) Protection	111	71	A2
ECVP-1	Virus Protection	112	71	A2
ECWN-1	Wireless Computing and Network	113	72	A2
EBCR-1	Connection Rules	114	72	A2
EBVC-1	VPN Controls	115	72	A2

IACN	IA Control Name	Appearance Index	Page	Attachment
PEEL-2	Emergency Lighting	116	72	A2
PEFD-2	Fire Detection	117	72	A2
PEFI-1	Fire Inspection	118	72	A2
PEFS-2	Fire Suppression	119	72	A2
PEHC-2	Humidity Controls	120	72	A2
PEMS-1	Master Power Switch	121	72	A2
PESL-1	Screen Lock	122	73	A2
PETC-2	Temperature Controls	123	73	A2
PETN-1	Environmental Control Training	124	73	A2
PEVR-1	Voltage Regulators	125	73	A2
PRRB-1	Security Rules of Behavior or Acceptable Use Policy	126	73	A2
COAS-2	Alternate Site Designation	127	73	A2
COBR-1	Protection of Backup and Restoration Assets	128	73	A2
CODB-2	Data Backup Procedures	129	73	A2
CODP-2	Disaster and Recovery Planning	130	74	A2
COEB-1	Enclave Boundary Defense	131	74	A2
COED-1	Scheduled Exercises and Drills	132	74	A2
COEF-2	Identification of Essential Functions	133	74	A2
COMS-2	Maintenance Support	134	74	A2
COPS-2	Power Supply	135	74	A2
COSP-1	Spares and Parts	136	74	A2
COSW-1	Backup Copies of Critical SW	137	74	A2
COTR-1	Trusted Recovery	138	74	A2
VIIR-1	Incident Response Planning	139	75	A2
VIVM-1	Vulnerability Management	140	75	A2
DCAR-1	Procedural Review	141	76	A3
DCBP-1	Best Security Practices	142	76	A3
DCCB-1	Control Board	143	76	A3
DCCS-1	Configuration Specifications	144	76	A3
DCCT-1	Compliance Testing	145	76	A3
DCDS-1	Dedicated IA Services	146	76	A3

IACN	IA Control Name	Appearance Index	Page	Attachment
DCFA-1	Functional Architecture for AIS Applications	147	77	A3
DCHW-1	HW Baseline	148	77	A3
DCID-1	Interconnection Documentation	149	77	A3
DCII-1	IA Impact Assessment	150	77	A3
DCIT-1	IA for IT Services	151	77	A3
DCMC-1	Mobile Code	152	78	A3
DCNR-1	Non-repudiation	153	78	A3
DCPD-1	Public Domain Software Controls	154	78	A3
DCPP-1	Ports, Protocols, and Services	155	78	A3
DCPR-1	CM Process	156	79	A3
DCSD-1	IA Documentation	157	79	A3
DCSL-1	System Library Management Controls	158	79	A3
DCSQ-1	Software Quality	159	79	A3
DCSS-1	System State Changes	160	79	A3
DCSW-1	SW Baseline	161	79	A3
IAKM-1	Key Management	162	80	A3
IATS-1	Token and Certificate Standards	163	80	A3
ECAT-1	Audit Trail, Monitoring, Analysis and Reporting	164	80	A3
ECCD-1	Changes to Data	165	80	A3
ECIM-1	Instant Messaging	166	80	A3
ECND-1	Network Device Controls	167	80	A3
ECPA-1	Privileged Account Control	168	80	A3
ECPC-1	Production Code Change Controls	169	80	A3
ECRG-1	Audit Reduction and Report Generation	170	81	A3
ECSC-1	Security Configuration Compliance	171	81	A3
ECSD-1	Software Development Change Controls	172	81	A3
ECTM-1	Transmission Integrity Controls	173	81	A3
ECTP-1	Audit Trail Protection	174	81	A3
ECVI-1	Voice-over-IP (VoIP) Protection	175	81	A3
ECVP-1	Virus Protection	176	81	A3
ECWN-1	Wireless Computing and Network	177	81	A3

IACN	IA Control Name	Appearance Index	Page	Attachment
EBCR-1	Connection Rules	178	82	A3
EBVC-1	VPN Controls	179	82	A3
PEEL-1	Emergency Lighting	180	82	A3
PEFD-1	Fire Detection	181	82	A3
PEFI-1	Fire Inspection	182	82	A3
PEFS-1	Fire Suppression	183	82	A3
PEHC-1	Humidity Controls	184	82	A3
PEMS-1	Master Power Switch	185	82	A3
PESL-1	Screen Lock	186	82	A3
PETC-1	Temperature Controls	187	83	A3
PETN-1	Environmental Control Training	188	83	A3
PEVR-1	Voltage Regulators	189	83	A3
PRRB-1	Security Rules of Behavior or Acceptable Use Policy	190	83	A3
COAS-1	Alternate Site Designation	191	83	A3
COBR-1	Protection of Backup and Restoration Assets	192	83	A3
CODB-1	Data Backup Procedures	193	83	A3
CODP-1	Disaster and Recovery Planning	194	83	A3
COEB-1	Enclave Boundary Defense	195	83	A3
COED-1	Scheduled Exercises and Drills	196	83	A3
COEF-1	Identification of Essential Functions	197	84	A3
COMS-1	Maintenance Support	198	84	A3
COPS-1	Power Supply	199	84	A3
COSP-1	Spares and Parts	200	84	A3
COSW-1	Backup Copies of Critical SW	201	84	A3
COTR-1	Trusted Recovery	202	84	A3
VIIR-1	Incident Response Planning	203	84	A3
VIVM-1	Vulnerability Management	204	84	A3
DCAS-1	Acquisition Standards	205	85	A4
DCSR-3	Specified Robustness – Basic	206	85	A4
DCSS-2	System State Changes	207	85	A4
IAGA-1	Group Authentication	208	85	A4

IACN	IA Control Name	Appearance Index	Page	Attachment
IAIA-2	Individual Identification and Authentication	209	86	A4
IAKM-3	Key Management	210	86	A4
ECAD-1	Affiliation Display	211	86	A4
ECAN-1	Access for Need-to-Know	212	87	A4
ECAR-3	Audit Record Content – Public Systems	213	87	A4
ECAT-2	Audit Trail, Monitoring, Analysis and Reporting	214	87	A4
ECCD-2	Changes to Data	215	88	A4
ECCM-1	COMSEC	216	88	A4
ECCR-2	Encryption for Confidentiality (Data at Rest)	217	88	A4
ECCR-3	Encryption for Confidentiality (Data at Rest)	218	88	A4
ECCT-2	Encryption for Confidentiality (Data at Transmit)	219	88	A4
ECIC-1	Interconnections among DoD Systems and Enclaves	220	88	A4
ECLC-1	Audit of Security Label Changes	221	88	A4
ECLO-2	Logon	222	88	A4
ECLP-1	Least Privilege	223	89	A4
ECML-1	Marking and Labeling	224	89	A4
ECMT-2	Conformance Monitoring and Testing	225	89	A4
ECNK-1	Encryption for Need-To-Know	226	89	A4
ECNK-2	Encryption for Need-To-Know	227	89	A4
ECRC-1	Resource Control	228	89	A4
ECRR-1	Audit Record Retention	229	90	A4
ECTB-1	Audit Trail Backup	230	90	A4
ECTC-1	Tempest Controls	231	90	A4
ECWM-1	Warning Message	232	90	A4
IAAC-1	Account Control	233	90	A4
EBBD-3	Boundary Defense	234	90	A4
EBRP-1	Remote Access for Privileged Functions	235	90	A4
EBRU-1	Remote Access for User Functions	236	91	A4
PECF-2	Access to Computing Facilities	237	91	A4
PECS-2	Clearing and Sanitizing	238	91	A4
PEDD-1	Destruction	239	91	A4

IACN	IA Control Name	Appearance Index	Page	Attachment
PEDI-1	Data Interception	240	91	A4
PEPF-2	Physical Protection of Facilities	241	91	A4
PEPS-1	Physical Security Testing	242	91	A4
PESP-1	Workplace Security Procedures	243	91	A4
PESS-1	Storage	244	92	A4
PEVC-1	Visitor Control to Computing Facilities	245	92	A4
PRAS-2	Access to Information	246	92	A4
PRMP-2	Maintenance Personnel	247	92	A4
PRNK-1	Access to Need-to-Know Information	248	92	A4
PRTN-1	Information Assurance Training	249	92	A4
DCAS-1	Acquisition Standards	250	93	A5
DCSR-2	Specified Robustness – Basic	251	93	A5
IAGA-1	Group Authentication	252	93	A5
IAIA-1	Individual Identification and Authentication	253	94	A5
ECAD-1	Affiliation Display	254	94	A5
ECAN-1	Access for Need-to-Know	255	95	A5
ECAR-2	Audit Record Content – Public Systems	256	95	A5
ECAT-1	Audit Trail, Monitoring, Analysis and Reporting	257	95	A5
ECCR-1	Encryption for Confidentiality (Data at Rest)	258	95	A5
ECCT-1	Encryption for Confidentiality (Data at Transmit)	259	95	A5
ECIC-1	Interconnections among DoD Systems and Enclaves	260	96	A5
ECLO-1	Logon	261	96	A5
ECLP-1	Least Privilege	262	96	A5
ECML-1	Marking and Labeling	263	96	A5
ECMT-1	Conformance Monitoring and Testing	264	96	A5
ECNK-1	Encryption for Need-To-Know	265	96	A5
ECRC-1	Resource Control	266	97	A5
ECRR-1	Audit Record Retention	267	97	A5
ECTC-1	Tempest Controls	268	97	A5
ECWM-1	Warning Message	269	97	A5
IAAC-1	Account Control	270	97	A5

IACN	IA Control Name	Appearance Index	Page	Attachment
EBBD-2	Boundary Defense	271	97	A5
EBPW-1	Public WAN Connection	272	97	A5
EBRP-1	Remote Access for Privileged Functions	273	98	A5
EBRU-1	Remote Access for User Functions	274	98	A5
PECF-1	Access to Computing Facilities	275	98	A5
PECS-1	Clearing and Sanitizing	276	98	A5
PEDI-1	Data Interception	277	98	A5
PEPF-1	Physical Protection of Facilities	278	98	A5
PEPS-1	Physical Security Testing	279	98	A5
PESP-1	Workplace Security Procedures	280	99	A5
PESS-1	Storage	281	99	A5
PEVC-1	Visitor Control to Computing Facilities	282	99	A5
PRAS-1	Access to Information	283	99	A5
PRMP-1	Maintenance Personnel	284	99	A5
PRNK-1	Access to Need-to-Know Information	285	99	A5
PRTN-1	Information Assurance Training	286	99	A5
DCAS-1	Acquisition Standards	287	100	A6
DCSR-1	Specified Robustness – Basic	288	100	A6
ECAR-1	Audit Record Content – Public Systems	289	100	A6
ECAT-1	Audit Trail, Monitoring, Analysis and Reporting	290	100	A6
ECLP-1	Least Privilege	291	101	A6
ECMT-1	Conformance Monitoring and Testing	292	101	A6
ECRR-1	Audit Record Retention	293	101	A6
ECWM-1	Warning Message	294	101	A6
EBBD-1	Boundary Defense	295	101	A6
EBPW-1	Public WAN Connection	296	101	A6
PRMP-1	Maintenance Personnel	297	102	A6
PRNK-1	Access to Need-to-Know Information	298	102	A6

Table 69 IACs, Sorted on Attachment within IA Control Number (IACN)

IACN	IA Control Name	Appearance Index	Page	Attachment
COAS-2	Alternate Site Designation	57	62	A1
COAS-2	Alternate Site Designation	127	73	A2
COAS-1	Alternate Site Designation	191	83	A3
COBR-1	Protection of Backup and Restoration Assets	58	62	A1
COBR-1	Protection of Backup and Restoration Assets	128	73	A2
COBR-1	Protection of Backup and Restoration Assets	192	83	A3
CODB-3	Data Backup Procedures	59	62	A1
CODB-2	Data Backup Procedures	129	73	A2
CODB-1	Data Backup Procedures	193	83	A3
CODP-3	Disaster and Recovery Planning	60	63	A1
CODP-2	Disaster and Recovery Planning	130	74	A2
CODP-1	Disaster and Recovery Planning	194	83	A3
COEB-2	Enclave Boundary Defense	61	63	A1
COEB-1	Enclave Boundary Defense	131	74	A2
COEB-1	Enclave Boundary Defense	195	83	A3
COED-2	Scheduled Exercises and Drills	62	63	A1
COED-1	Scheduled Exercises and Drills	132	74	A2
COED-1	Scheduled Exercises and Drills	196	83	A3
COEF-2	Identification of Essential Functions	63	63	A1
COEF-2	Identification of Essential Functions	133	74	A2
COEF-1	Identification of Essential Functions	197	84	A3
COMS-2	Maintenance Support	64	63	A1
COMS-2	Maintenance Support	134	74	A2
COMS-1	Maintenance Support	198	84	A3
COPS-3	Power Supply	65	63	A1
COPS-2	Power Supply	135	74	A2
COPS-1	Power Supply	199	84	A3
COSP-2	Spares and Parts	66	63	A1
COSP-1	Spares and Parts	136	74	A2

IACN	IA Control Name	Appearance Index	Page	Attachment
COSP-1	Spares and Parts	200	84	A3
COSW-1	Backup Copies of Critical SW	67	63	A1
COSW-1	Backup Copies of Critical SW	137	74	A2
COSW-1	Backup Copies of Critical SW	201	84	A3
COTR-1	Trusted Recovery	68	63	A1
COTR-1	Trusted Recovery	138	74	A2
COTR-1	Trusted Recovery	202	84	A3
DCAR-1	Procedural Review	1	54	A1
DCAR-1	Procedural Review	71	65	A2
DCAR-1	Procedural Review	141	76	A3
DCAS-1	Acquisition Standards	205	85	A4
DCAS-1	Acquisition Standards	250	93	A5
DCAS-1	Acquisition Standards	287	100	A6
DCBP-1	Best Security Practices	2	54	A1
DCBP-1	Best Security Practices	72	65	A2
DCBP-1	Best Security Practices	142	76	A3
DCCB-2	Control Board	3	54	A1
DCCB-2	Control Board	73	65	A2
DCCB-1	Control Board	143	76	A3
DCCS-2	Configuration Specifications	4	54	A1
DCCS-2	Configuration Specifications	74	65	A2
DCCS-1	Configuration Specifications	144	76	A3
DCCT-1	Compliance Testing	5	54	A1
DCCT-1	Compliance Testing	75	65	A2
DCCT-1	Compliance Testing	145	76	A3
DCDS-1	Dedicated IA Services	6	54	A1
DCDS-1	Dedicated IA Services	76	65	A2
DCDS-1	Dedicated IA Services	146	76	A3
DCFA-1	Functional Architecture for AIS Applications	7	55	A1
DCFA-1	Functional Architecture for AIS Applications	147	77	A3
DCFA-1	Functional Architecture for AIS Applications	77	66	A2

IACN	IA Control Name	Appearance Index	Page	Attachment
DCHW-1	HW Baseline	8	55	A1
DCHW-1	HW Baseline	78	66	A2
DCHW-1	HW Baseline	148	77	A3
DCID-1	Interconnection Documentation	9	55	A1
DCID-1	Interconnection Documentation	79	66	A2
DCID-1	Interconnection Documentation	149	77	A3
DCII-1	IA Impact Assessment	10	55	A1
DCII-1	IA Impact Assessment	80	66	A2
DCII-1	IA Impact Assessment	150	77	A3
DCIT-1	IA for IT Services	11	55	A1
DCIT-1	IA for IT Services	81	66	A2
DCIT-1	IA for IT Services	151	77	A3
DCMC-1	Mobile Code	12	56	A1
DCMC-1	Mobile Code	82	67	A2
DCMC-1	Mobile Code	152	78	A3
DCNR-1	Non-repudiation	13	56	A1
DCNR-1	Non-repudiation	83	67	A2
DCNR-1	Non-repudiation	153	78	A3
DCPA-1	Partitioning the Application	14	56	A1
DCPA-1	Partitioning the Application	84	67	A2
DCPB-1	IA Program and Budget	15	56	A1
DCPB-1	IA Program and Budget	85	67	A2
DCPD-1	Public Domain Software Controls	16	57	A1
DCPD-1	Public Domain Software Controls	86	68	A2
DCPD-1	Public Domain Software Controls	154	78	A3
DCPP-1	Ports, Protocols, and Services	17	57	A1
DCPP-1	Ports, Protocols, and Services	87	68	A2
DCPP-1	Ports, Protocols, and Services	155	78	A3
DCPR-1	CM Process	18	57	A1
DCPR-1	CM Process	88	68	A2
DCPR-1	CM Process	156	79	A3

IACN	IA Control Name	Appearance Index	Page	Attachment
DCSD-1	IA Documentation	19	57	A1
DCSD-1	IA Documentation	89	68	A2
DCSD-1	IA Documentation	157	79	A3
DCSL-1	System Library Management Controls	20	57	A1
DCSL-1	System Library Management Controls	90	69	A2
DCSL-1	System Library Management Controls	158	79	A3
DCSP-1	Security Support Structure Partitioning	21	58	A1
DCSP-1	Security Support Structure Partitioning	91	69	A2
DCSQ-1	Software Quality	22	58	A1
DCSQ-1	Software Quality	92	69	A2
DCSQ-1	Software Quality	159	79	A3
DCSR-3	Specified Robustness – Basic	206	85	A4
DCSR-2	Specified Robustness – Basic	251	93	A5
DCSR-1	Specified Robustness – Basic	288	100	A6
DCSS-2	System State Changes	23	58	A1
DCSS-2	System State Changes	93	69	A2
DCSS-1	System State Changes	160	79	A3
DCSS-2	System State Changes	207	85	A4
DCSW-1	SW Baseline	24	58	A1
DCSW-1	SW Baseline	94	69	A2
DCSW-1	SW Baseline	161	79	A3
EBBD-3	Boundary Defense	234	90	A4
EBBD-2	Boundary Defense	271	97	A5
EBBD-1	Boundary Defense	295	101	A6
EBCR-1	Connection Rules	44	61	A1
EBCR-1	Connection Rules	114	72	A2
EBCR-1	Connection Rules	178	82	A3
EBPW-1	Public WAN Connection	272	97	A5
EBPW-1	Public WAN Connection	296	101	A6
EBRP-1	Remote Access for Privileged Functions	235	90	A4
EBRP-1	Remote Access for Privileged Functions	273	98	A5

IACN	IA Control Name	Appearance Index	Page	Attachment
EBRU-1	Remote Access for User Functions	236	91	A4
EBRU-1	Remote Access for User Functions	274	98	A5
EBVC-1	VPN Controls	45	61	A1
EBVC-1	VPN Controls	115	72	A2
EBVC-1	VPN Controls	179	82	A3
ECAD-1	Affiliation Display	211	86	A4
ECAD-1	Affiliation Display	254	94	A5
ECAN-1	Access for Need-to-Know	212	87	A4
ECAN-1	Access for Need-to-Know	255	95	A5
ECAR-3	Audit Record Content – Public Systems	213	87	A4
ECAR-2	Audit Record Content – Public Systems	256	95	A5
ECAR-1	Audit Record Content – Public Systems	289	100	A6
ECAT-2	Audit Trail, Monitoring, Analysis and Reporting	27	58	A1
ECAT-2	Audit Trail, Monitoring, Analysis and Reporting	97	69	A2
ECAT-1	Audit Trail, Monitoring, Analysis and Reporting	164	80	A3
ECAT-2	Audit Trail, Monitoring, Analysis and Reporting	214	87	A4
ECAT-1	Audit Trail, Monitoring, Analysis and Reporting	257	95	A5
ECAT-1	Audit Trail, Monitoring, Analysis and Reporting	290	100	A6
ECCD-2	Changes to Data	28	58	A1
ECCD-2	Changes to Data	98	70	A2
ECCD-1	Changes to Data	165	80	A3
ECCD-2	Changes to Data	215	88	A4
ECCM-1	COMSEC	216	88	A4
ECCR-2	Encryption for Confidentiality (Data at Rest)	217	88	A4
ECCR-3	Encryption for Confidentiality (Data at Rest)	218	88	A4
ECCR-1	Encryption for Confidentiality (Data at Rest)	258	95	A5
ECCT-2	Encryption for Confidentiality (Data at Transmit)	219	88	A4
ECCT-1	Encryption for Confidentiality (Data at Transmit)	259	95	A5
ECDC-1	Data Change Controls	29	59	A1
ECDC-1	Data Change Controls	99	70	A2
ECIC-1	Interconnections among DoD Systems and Enclaves	220	88	A4

IACN	IA Control Name	Appearance Index	Page	Attachment
ECIC-1	Interconnections among DoD Systems and Enclaves	260	96	A5
ECID-1	Host Based IDS	30	59	A1
ECID-1	Host Based IDS	100	70	A2
ECIM-1	Instant Messaging	31	59	A1
ECIM-1	Instant Messaging	101	70	A2
ECIM-1	Instant Messaging	166	80	A3
ECLC-1	Audit of Security Label Changes	221	88	A4
ECLO-2	Logon	222	88	A4
ECLO-1	Logon	261	96	A5
ECLP-1	Least Privilege	223	89	A4
ECLP-1	Least Privilege	262	96	A5
ECLP-1	Least Privilege	291	101	A6
ECML-1	Marking and Labeling	224	89	A4
ECML-1	Marking and Labeling	263	96	A5
ECMT-2	Conformance Monitoring and Testing	225	89	A4
ECMT-1	Conformance Monitoring and Testing	264	96	A5
ECMT-1	Conformance Monitoring and Testing	292	101	A6
ECND-2	Network Device Controls	32	59	A1
ECND-2	Network Device Controls	102	70	A2
ECND-1	Network Device Controls	167	80	A3
ECNK-1	Encryption for Need-To-Know	226	89	A4
ECNK-2	Encryption for Need-To-Know	227	89	A4
ECNK-1	Encryption for Need-To-Know	265	96	A5
ECPA-1	Privileged Account Control	33	59	A1
ECPA-1	Privileged Account Control	103	70	A2
ECPA-1	Privileged Account Control	168	80	A3
ECPC-2	Production Code Change Controls	34	59	A1
ECPC-2	Production Code Change Controls	104	70	A2
ECPC-1	Production Code Change Controls	169	80	A3
ECRC-1	Resource Control	228	89	A4
ECRC-1	Resource Control	266	97	A5

IACN	IA Control Name	Appearance Index	Page	Attachment
ECRG-1	Audit Reduction and Report Generation	35	59	A1
ECRG-1	Audit Reduction and Report Generation	105	70	A2
ECRG-1	Audit Reduction and Report Generation	170	81	A3
ECRR-1	Audit Record Retention	229	90	A4
ECRR-1	Audit Record Retention	267	97	A5
ECRR-1	Audit Record Retention	293	101	A6
ECSC-1	Security Configuration Compliance	36	59	A1
ECSC-1	Security Configuration Compliance	106	71	A2
ECSC-1	Security Configuration Compliance	171	81	A3
ECSD-2	Software Development Change Controls	37	60	A1
ECSD-2	Software Development Change Controls	107	71	A2
ECSD-1	Software Development Change Controls	172	81	A3
ECTB-1	Audit Trail Backup	38	60	A1
ECTB-1	Audit Trail Backup	108	71	A2
ECTB-1	Audit Trail Backup	230	90	A4
ECTC-1	Tempest Controls	231	90	A4
ECTC-1	Tempest Controls	268	97	A5
ECTM-2	Transmission Integrity Controls	39	60	A1
ECTM-2	Transmission Integrity Controls	109	71	A2
ECTM-1	Transmission Integrity Controls	173	81	A3
ECTP-1	Audit Trail Protection	40	60	A1
ECTP-1	Audit Trail Protection	110	71	A2
ECTP-1	Audit Trail Protection	174	81	A3
ECVI-1	Voice-over-IP (VoIP) Protection	41	60	A1
ECVI-1	Voice-over-IP (VoIP) Protection	111	71	A2
ECVI-1	Voice-over-IP (VoIP) Protection	175	81	A3
ECVP-1	Virus Protection	42	60	A1
ECVP-1	Virus Protection	112	71	A2
ECVP-1	Virus Protection	176	81	A3
ECWM-1	Warning Message	232	90	A4
ECWM-1	Warning Message	269	97	A5

IACN	IA Control Name	Appearance Index	Page	Attachment
ECWM-1	Warning Message	294	101	A6
ECWN-1	Wireless Computing and Network	43	60	A1
ECWN-1	Wireless Computing and Network	113	72	A2
ECWN-1	Wireless Computing and Network	177	81	A3
IAAC-1	Account Control	233	90	A4
IAAC-1	Account Control	270	97	A5
IAGA-1	Group Authentication	208	85	A4
IAGA-1	Group Authentication	252	93	A5
IAIA-2	Individual Identification and Authentication	209	86	A4
IAIA-1	Individual Identification and Authentication	253	94	A5
IAKM-2	Key Management	25	58	A1
IAKM-2	Key Management	95	69	A2
IAKM-1	Key Management	162	80	A3
IAKM-3	Key Management	210	86	A4
IATS-2	Token and Certificate Standards	26	58	A1
IATS-2	Token and Certificate Standards	96	69	A2
IATS-1	Token and Certificate Standards	163	80	A3
PECF-2	Access to Computing Facilities	237	91	A4
PECF-1	Access to Computing Facilities	275	98	A5
PECS-2	Clearing and Sanitizing	238	91	A4
PECS-1	Clearing and Sanitizing	276	98	A5
PEDD-1	Destruction	239	91	A4
PEDI-1	Data Interception	240	91	A4
PEDI-1	Data Interception	277	98	A5
PEEL-2	Emergency Lighting	46	61	A1
PEEL-2	Emergency Lighting	116	72	A2
PEEL-1	Emergency Lighting	180	82	A3
PEFD-2	Fire Detection	47	61	A1
PEFD-2	Fire Detection	117	72	A2
PEFD-1	Fire Detection	181	82	A3
PEFI-1	Fire Inspection	48	61	A1

IACN	IA Control Name	Appearance Index	Page	Attachment
PEFI-1	Fire Inspection	118	72	A2
PEFI-1	Fire Inspection	182	82	A3
PEFS-2	Fire Suppression	49	61	A1
PEFS-2	Fire Suppression	119	72	A2
PEFS-1	Fire Suppression	183	82	A3
PEHC-2	Humidity Controls	50	61	A1
PEHC-2	Humidity Controls	120	72	A2
PEHC-1	Humidity Controls	184	82	A3
PEMS-1	Master Power Switch	51	61	A1
PEMS-1	Master Power Switch	121	72	A2
PEMS-1	Master Power Switch	185	82	A3
PEPF-2	Physical Protection of Facilities	241	91	A4
PEPF-1	Physical Protection of Facilities	278	98	A5
PEPS-1	Physical Security Testing	242	91	A4
PEPS-1	Physical Security Testing	279	98	A5
PESL-1	Screen Lock	52	62	A1
PESL-1	Screen Lock	122	73	A2
PESL-1	Screen Lock	186	82	A3
PESP-1	Workplace Security Procedures	243	91	A4
PESP-1	Workplace Security Procedures	280	99	A5
PESS-1	Storage	244	92	A4
PESS-1	Storage	281	99	A5
PETC-2	Temperature Controls	53	62	A1
PETC-2	Temperature Controls	123	73	A2
PETC-1	Temperature Controls	187	83	A3
PETN-1	Environmental Control Training	54	62	A1
PETN-1	Environmental Control Training	124	73	A2
PETN-1	Environmental Control Training	188	83	A3
PEVC-1	Visitor Control to Computing Facilities	245	92	A4
PEVC-1	Visitor Control to Computing Facilities	282	99	A5
PEVR-1	Voltage Regulators	55	62	A1

IACN	IA Control Name	Appearance Index	Page	Attachment
PEVR-1	Voltage Regulators	125	73	A2
PEVR-1	Voltage Regulators	189	83	A3
PRAS-2	Access to Information	246	92	A4
PRAS-1	Access to Information	283	99	A5
PRMP-2	Maintenance Personnel	247	92	A4
PRMP-1	Maintenance Personnel	284	99	A5
PRMP-1	Maintenance Personnel	297	102	A6
PRNK-1	Access to Need-to-Know Information	248	92	A4
PRNK-1	Access to Need-to-Know Information	285	99	A5
PRNK-1	Access to Need-to-Know Information	298	102	A6
PRRB-1	Security Rules of Behavior or Acceptable Use Policy	56	62	A1
PRRB-1	Security Rules of Behavior or Acceptable Use Policy	126	73	A2
PRRB-1	Security Rules of Behavior or Acceptable Use Policy	190	83	A3
PRTN-1	Information Assurance Training	249	92	A4
PRTN-1	Information Assurance Training	286	99	A5
VIIR-2	Incident Response Planning	69	64	A1
VIIR-1	Incident Response Planning	139	75	A2
VIIR-1	Incident Response Planning	203	84	A3
VIVM-1	Vulnerability Management	70	64	A1
VIVM-1	Vulnerability Management	140	75	A2
VIVM-1	Vulnerability Management	204	84	A3

9 DISTRIBUTION

1	MS 0899	RIM-Reports Management	9532 (electronic copy)
1	MS 0260	D.R. White	5620
1	MS 0672	M. Shakamuri	5621
1	MS0672	P.L. Campbell	5629
1	MS 0672	H.W. Lin	5629
1	MS 1002	J.E. Nelson	6520
1	MS 0780	J. Eberhart	6521
1	MS 0785	I.C. Alexander	6523
1	MS 0780	D.A. Pritchard	6524
1	MS 0781	C.B. Richardson	6525
1	MS 0785	E.L. Witzke	6525