Preface

As the federal regulators have come to understand the risks to the U.S. national infrastructure, regulations and laws have been written to ensure that due diligence occurs in securing critical applications and systems. An outcome of the laws and regulations is a formalized process for reviewing, documenting, analyzing, and evaluating information security requirements and controls. The process described in this book, known as C&A, will assist government agencies in complying with the Federal Information Security Management Act of 2002.

Audience

The audience for this book includes those individuals currently performing information security support at U.S. Federal agencies, defense contractors that need to comply with FISMA to support government task orders, information security consultants, and anyone else who would like to learn a very thorough methodology for conducting information security audits to safeguard sensitive information, mission-critical applications, and their underlying infrastructure.

While much of the discussion in this book is geared to U.S. federal agencies, this book describes a process that can essentially be applied to any information technology organizations or infrastructure. This book does not describe the only way to perform C&A; however, it does describe a methodology that has been proven successful in assisting U.S. government agencies in obtaining near-perfect scores on the annual Federal Computer Security Report Card. All kinds of variations for performing C&A exist. This book describes one way.

Organization of This Book

This book contains 24 chapters.

Chapter 1 (*What Is Certification and Accreditation?*) explains what is meant by Certification and Accreditation and why the process is mandated by federal law. The different Certification and Accreditation laws will be cited and discussed. A brief history and chronology of the mandated laws will be included in the discussion.

Chapter 2 (*Types of Certification and Accreditation*) includes descriptions of the four primary different types of C&A: NIST, NIACAP, DITSCAP, and DCID 6/3.

Chapter 3 (*Understanding the Certification and Accreditation Process*) explains the logical steps that one goes through to prepare for a C&A audit/review. It also explains the roles and responsibilities of the audit/review team, including the role of the reviewers, the accrediting authority, and the federal auditors/inspectors.

Chapter 4 (*Establishing a Certification and Accreditation Program*) includes information on what types of tasks you'll need to do to put a C&A Program into place. This chapter explains what types of documents and guidelines you'll need to establish a C&A Program. If you already have a C&A Program, you can always make it better and refine it. You'll want to improve your C&A Program and revise it periodically as you notice what items are missing and what areas need more clarification.

Chapter 5 (*Developing a Certification Package*) includes information on what you need to do to prepare for an upcoming C&A project. This chapter tells you what documents you need to collect and have on hand in order to prepare your C&A review (e.g., the organizational security policies and procedures and the security organization structure). Information on whether to outsource the C&A review or do it in-house is also provided.

Chapter 6 (*Preparing the Hardware and Software Inventory*) includes a sample of a C&A asset inventory and how one should go about developing it and putting it together.

Chapter 7 (*Determining the Certification Level*) includes information on how to put together the *Security Categorization and Certification Level* approval letter and the *Determination Level Profile* documents.

Chapter 8 (*Performing and Preparing the Self-Assessment*) includes information on how to perform and document a Self-Assessment. The differences between management, operational, and technical security controls are explained.

Chapter 9 (*Addressing Security Awareness and Training Requirements*) includes information on how to review, analyze, and document Security Awareness, Training, and Education.

Chapter 10 (*Addressing End-User Rules of Behavior*) advises you on how to review, analyze, and document C&A requirements for *End-User Rules of Behavior*.

Chapter 11 (*Addressing Incident Response*) includes information on how to address and document Incident Response requirements. The role of the incident response manager and different incident types are discussed.

Chapter 12 (*Performing the Security Tests and Evaluation*) includes information on how to perform and document the required security tests and evaluation (ST&E). This chapter also addresses whether or not a penetration test is required. Information about how to execute a penetration test will be discussed.

Chapter 13 (*Conducting a Privacy Impact Assessment*) helps you understand under what circumstances you'll need to develop one of these types of documents and what to include in one. Individual privacy rights and responsibilities of the Senior Agency Official for Privacy are discussed.

Chapter 14 (*Performing the Business Risk Assessment*) includes information on how to perform a *Business Risk Assessment* and what types of information should be included in a *Business Risk Assessment*.

Chapter 15 (*Preparing the Business Impact Assessment*) includes information on how to prepare and perform the *Business Impact Assessment* and what types of information should be included in such an assessment.

Chapter 16 (*Developing the Contingency Plan*) includes information on how to prepare a *Contingency Plan* and what types of information should be included in a *Contingency Plan*.

Chapter 17 (*Performing a System Risk Assessment*) includes information on how to prepare and perform the *System Risk Assessment*.

Chapter 18 (*Developing a Configuration Management Plan*) explains what you'll want to include in this plan, and how to go about accumulating the information.

Chapter 19 (*Preparing the System Security Plan*) includes how to prepare and document a *System Security Plan*.

Chapter 20 (*Submitting the C&A Package*) includes information on how to put together the final Certification Package. Information on the *Security Assessment Report* prepared by the Certifying Agent is also included in this chapter.

Chapter 21 (*Evaluating the Certification Package for Accreditation*) includes information on how to evaluate a Certification Package to determine if it should be accredited. This chapter includes information on how the evaluators determine whether the package should pass or fail. Checklists and how to use them to produce the *Security Assessment Report* are discussed.

Chapter 22 (*Addressing C&A Findings*) includes information on strategies for defending your C&A review, as well as how to address any failures cited by the evaluation team. The evaluators typically require a document known as a *Plan of Action & Milestones (POA&M)* to be drafted and adhered to for the purpose of addressing failures. A sample *POA&M* is included along with recommendations on how to write one.

Chapter 23 (*Improving Your Federal Computer Security Report Card Scores*) explains what shows up in the FISMA Report Cards and how to go about improving your agency's scores.

Chapter 24 (*Resources*) includes a list of recommended resources that C&A teams can use to help understand the C&A process. A list of acromyns is also included

Conventions Used in This Book

The following typographical conventions are used in this book:

Italic is used for commands, directory names, filenames, scripts, emphasis, and the first use of technical terms.

Bold is used for emphasis.

Arrow < brackets > are used for user input.

We'd Like to Hear From You

We have reviewed and verified all of the information in this book to the best of our ability, but you may find that certain references to federal regulations have changed.

For more information about this book and others, see the Syngress Web site: www.syngress.com/solutions.com.

Author Acknowledgments

Without the help and support of many individuals, this book would not have been possible. I'd like to thank my editors, Gary Byrne and Matthew Shepherd, who helped keep me on track and polished up the rough edges. I'd also like to thank Andrew Williams for giving me the opportunity to write for Syngress. The entire Syngress team is a world-class publishing organization. I'd also like to thank my former editors at O'Reilly Media, Allison Randal and Tatiana Apandi Diaz, who helped me refine some of the earlier drafts of this book. Thank you also to Nathan Torkington of O'Reilly, who was one of the early believers in this book.

Thank you to Stephen Northcutt of SANS, who was instrumental in helping this book get off the ground.

Various C&A and security professionals whom I have worked with over the years have all contributed to my knowledge of C&A, which likely resulted in a better book. Various people provided research for this book, and some even allowed me to C&A their mission-critical systems, which no matter how many times I do it, never fails to add new learning experiences. Alphabetically by last name, I'd like to thank John Alger, Gwen Bryant-Hill, Chris Buehler, John Cowan, Tamiiko Emery, Whitney Goss, Sheila Higgs, Cindi Jansohn, Yi-Fang Koh, Dave Metler, Angela Rivera, and Angela Vessels.

Thank you to Wanda Headley at the Natural Hazards Center at the University of Colorado, Boulder, for help with research on natural hazards. I'd also like to thank Eileen McVey, of the National Oceanic & Atmospheric Administration, who contributed information on natural hazard probabilities.

Thank you to the staff at COACT for all the support and words of encouragement. In particular, I'd like to thank Jim McGehee, Lou Lauer, Randy Williams, and Glenn Jacoboson, who made contributions to Chapter 22.

Thank you to Micah Tapman of SAIC, who provided research and recommendations for Chapter 23.

Thank you to Brien Posey, Shaam Rodrigo, and Troy Thompson of Relevant Technologies. They are consistently always there when I need an extra helping hand.

Much thanks to my parents, Barbara and Robert Taylor, who made many sacrifices to help me receive the education that gave me a foundation for writing.

Last, and most of all, I'd like to thank my 13-year-old son, Sammy, who gave up numerous hours of family time with Mom to make this book possible.

—Laura Taylor
Columbia, MD
October 2006