FROM THE PUZZLE OF MANY TO THE CLARITY OF ONE

IC INTEGRATION IN BADGE INTEROPERABILITY

CSNR LESSONS LEARNED SERIES

CSNR LESSONS LEARNED SERIES

From the Puzzle of Many to the Clarity of One

IC INTEGRATION IN BADGE INTEROPERABILITY

CENTER FOR THE STUDY OF
NATIONAL RECONNAISSANCE

JULY 2009

National Security Information

Unauthorized Disclosure Subject to Criminal Sanctions

The Center for the Study of National Reconnaissance (CSNR) is an independent NRO research body reporting to the NRO Deputy Director, Business Plans and Operations. Its primary objective is to ensure that the NRO leadership has the analytic framework and historical context to make effective policy and programmatic decisions. The CSNR accomplishes its mission by promoting the study, dialogue, and understanding of the discipline, practice, and history of national reconnaissance. The Center studies the past, analyzes the present, searches for lessons-learned.

How to obtain CSNR Publications: Call [redacted] secure or [redacted] on the open line; or email [redacted] on the classified intranet or csnr-nro@nro.mil. (b)(3)

Published by
National Reconnaissance Office
14675 Lee Road
Chantilly, Virginia 20151-1715

Printed in the United States of America

Table of Contents

Foreword

The success of the first phase of the Intelligence Community (IC) badge interoperability program in 2007 — after two unsuccessful attempts between 1970 and 2000 — offers numerous lessons for security and information technology activities, as well as insight into IC integration and collaboration actions. This lessons-learned monograph presents an account of the badge interoperability program's origins and development, as well as the first detailed history of the earlier Apex program and IC badge reciprocity attempts. In addition to being a report for security specialists about collaborative integration of a security process, it also is a report for all those in the IC who are faced with challenges related to interagency collaboration and technological integration.

In 2005 the Director of National Intelligence's (DNI's) *National Intelligence Strategy* called upon our community of intelligence officers within the IC to "Learn from our successes and mistakes to anticipate and be ready for new challenges."[1] Both successes and mistakes are part of being human — and a part of learning. If individuals and organizations are to develop successfully, they need to be aware of where and why they have been successful and made mistakes. Both of these kind of experiences are opportunities to learn. They are opportunities to reflect on past behaviors, identify alternative courses of action, and integrate those alternate behaviors into new ways of conducting business for the future. The rigorous analysis of past behavior — based on documented facts as we have attempted to do is this study — is an integral part of learning. It is in that spirit that we have undertaken this project.

We in the Center for the Study of National Reconnaissance (CSNR) are grateful to the Intelligence Community Lessons Learned Center (IC LLC) in the Office of the Director of National Intelligence for funding this study under its 2007 Lessons Learned Awareness Program. This competitive program awarded funding that would assist the Intelligence Community with incorporating lessons learned activities into its current and future activities.

Ms. Mary Rose McCaffrey, the former Director of the NRO Office of Security and Counterintelligence (OS&CI), and I worked together to enable this joint study. She proposed the idea, and together we tapped into the subject matter expertise and functional strengths of our respective offices. During the project, the CSNR's Research, Studies, & Analysis (RSA) Section monitored the research to ensure that it met social-science research standards and reflected a Community-level, rather than NRO-centric perspective.

The primary author of this study [redacted] formerly an employee of Booz Allen Hamilton, was an ideal candidate to lead the study. She had supported NRO's OS&CI as an organizational analyst from 2002-2008, is knowledgeable in organizational development matters, and holds a Master of Arts degree from Marymount University. Her Bachelor of Science degree is from Cornell University. She currently conducts lessons-learned analyses for the Intelligence Community in the Center for the Study of National Reconnaissance as an employee of Innovative Analytics and Training, LLC. (b)(3)

[1] Enterprise Objective 9 in the *National Intelligence Strategy*.

I join the research team in acknowledging the pioneering spirit that the IC agency leaders, their senior security managers, and the community's security and information technology specialists played in shepherding badge interoperability from concept to reality. As you read this monograph, I invite you to consider how this collaborative Community approach to integrating technologies can serve as a model, not just for the security and information technology domains, but for all domains across the Intelligence Community.

ROBERT A. MCDONALD, PH.D.
Director, Center for the Study of National Reconnaissance
Business Plans and Operations
National Reconnaissance Office

Preface

This monograph describes the operational debut of a long-desired goal — the interoperable Intelligence Community (IC) badge. Phase One of the IC badge interoperability program, from its inception in 2003 to its completion in 2007, represents a major success for the IC: the agencies overcame security and information technology differences to achieve shared goals. This study also documents two previous chapters in badge history — one from the 1970s and a second from the 1990s. When we compared badge interoperability to these earlier chapters, we noticed patterns that suggest systemic obstacles hampered implementation of a community badge, not any one leader or agency.

We interviewed subject matter experts from each agency that participated in Phase One of badge interoperability. In addition, security officers involved with the 1970s' and 1990s' chapters helped outline those events to support future research. The pages that follow draw from archival records, internal communications, and existing histories from various agencies and open sources.

The written record provides a more limited perspective. Interviewees voluntarily offered copies of briefings, reports, and other documents for badge interoperability (2003-2007). We reviewed archival material from NRO and NSA for Apex and badge reciprocity records. The CIA and DIA did not provide archival material, and because NGA did not exist in its current form during these earlier chapters, we did not pursue NGA archives. Future research of CIA and DIA archives will produce a more balanced view.

This study would not have been possible without the support of many others. The IC Lessons Learned Center approved this study proposal, provided funding, and lent their support. Robert A. McDonald, Ph.D. (Director, the Center for the Study of National Reconnaissance) and Susan D. Schultz, Ph.D. (Chief of the Research, Studies, & Analysis Section of CSNR) provided endless guidance to shape the research and this report. Ms. Sharon Moreno [redacted] (b)(3)
[redacted] (b)(3) from CSNR provided copy editing assistance.

I extend thanks to Ms. Mary Rose McCaffrey, former Director of the NRO Office of Security and Counterintelligence, for initiating the study proposal and providing steady support to the project. The Intelligence Community Badge Interoperability Program (ICBIP) Program Manager and members of the Access Control Working Group (ACWG) generously gave us their time and shared their insights. In addition, two researchers helped define the study concept, conduct the research, and develop this written history and findings — thank you to [redacted] (b)(3)

Anything good in this report comes from their assistance. All errors or omissions remain my responsibility. I hope you find this study helpful in understanding how underlying security and technology requirements complicate interagency programs, and will apply these lessons to other programs you work in the future.

[redacted] (b)(3)

18 June 2009

Introduction

> *"Those {the 9/11} attacks showed, emphatically, that ways of doing business rooted in a different era are just not good enough. Americans should not settle for incremental, ad hoc adjustments to a system designed generations ago for a world that no longer exists."*
>
> *—9/11 Commission, p. 399*

In the decades following the establishment of the U.S. Intelligence Community (IC) with the National Security Act of 1947, there have been numerous efforts to reform and streamline how the U.S. collects and analyzes foreign intelligence. However, it was not until the tragic events of September 11, 2001 — when Al-Qae'da drove commercial airplanes into New York's World Trade Towers and the Pentagon, killing thousands of innocent civilians in a surprise attack — that the U.S. Congress mandated and enacted legislation geared toward major reform of U.S. intelligence.

At the core of the criticisms prompting intelligence reform was the belief that the IC's failure in information sharing — failure in "connecting the dots" — was at the root of the U.S.'s inability to warn of/or prevent the attack in the months prior to September 11 (9/11 Commission, 2004, p. 399). Similarly, the architects of the *WMD Commission* (2005) argued that the intelligence "failure" *vis-à-vis* weapons of mass destruction (Iraq) was attributable to the fact that the IC had been "fragmented," concluding that integration must be at the forefront of intelligence reform (WMD Commission, 2005, p. 309).

The tragic events of 9/11 constituted a shocking national security imperative that — finally in 2003 — provided the kind of impetus needed for the IC to establish a common badge for at least five agencies (the Central Intelligence Agency, the National Reconnaissance Office, the National Security Agency, the Defense Intelligence Agency, and the National Geospatial Agency). In one sense, the ability to implement a common badge provided concrete evidence that a post-9/11 Intelligence Community was indeed capable of reforming itself, and was serious about addressing scathing public and Congressional critique.

However, a common badge — allowing officers to share information more easily by facilitating easy passage among agencies without the laborious process of passing clearances — was hardly a new idea. Indeed, nearly four decades earlier — during the 1970s when the CIA's activities had provoked unprecedented criticism and fueled public and U.S. Congressional calls for reform in the IC — Admiral Stansfield Turner, Director of Central Intelligence (DCI) under President Jimmy Carter, established a program (Apex) designed to resolve the security structures and processes perceived as impediments to an effective IC, to include the implementation of a common badge. Similarly during the 1990s, the IC initiated badge reciprocity with the intention of fostering cooperation among the various intelligence agencies.

In short, neither the idea of nor the need for badge interoperability were new. But it was only after the tragic events of 9/11 that members of the IC had the requisite will and the sense of a common mission that enabled them to overcome the real obstacles hindering greater intelligence agency cooperation. It was this will at the working level — rather than leadership or bureaucratic restructuring *per se* — that was pivotal to integrating CIA, NRO, NSA, NGA, and DIA into one common badge (Phase One of the Badge Interoperability Program). Indeed, DCI George Tenet initiated badge interoperability in October 2003, nearly a year before the U.S. Congress enacted the Intelligence Reform and Terrorism Prevention Act (December 2004).

It has been more than seven years since the tragic events of that fateful day. Much hard work remains to be done. Eleven agencies are still to be incorporated into a common IC badge. Most officers of the 16 agencies comprising the U.S. Intelligence Community are involved in numerous other initiatives aimed at fostering collaboration — for example, attempting to standardize a classification guide, reform security clearance policies and processes, increase classified connectivity, reform analytic practices, and streamline the IC's collection capabilities. None of these initiatives are easy. But implementing a common badge for CIA, NRO, NGA, NSA, and DIA was not always easy: intelligence officers responsible for implementing badge interoperability also faced numerous obstacles. How they successfully dealt with obstacles and persisted despite lack of dedicated funding and staff between 2003 and 2007 has a great deal to teach us as we face the challenges of today.

SUSAN D. SCHULTZ, PH.D.
Chief/Research, Studies, & Analysis Section
Center for the Study of National Reconnaissance

Executive Summary

In October 2003, the Director of Central Intelligence (DCI) charged five Intelligence Community (IC) agencies — CIA, DIA, NGA, NRO, and NSA — with making their badges interoperable. The goal was to provide all employees of these five agencies with a common badge that would enable them to use their badges, along with a personal identification number, to gain physical access to any of the five agencies. There would be no requirement to pass security clearances or obtain visitor certifications. These five agencies overcame several obstacles and successfully achieved this goal. The Director of National Intelligence (DNI) announced completion of Phase One of the Intelligence Community Badge Interoperability Program in April 2007. [2]

This monograph provides insight on the implementation of Phase One of this long-desired goal of an interoperable IC badge.

Lessons Learned: From our assessment of the experiences of those involved with Phase One of Badge Interoperability, we learned five major lessons:

- When the Intelligence Community (IC) commits to addressing a well-defined need, success for an interagency program is more likely.
- When full project complexities are not considered during initial planning, deadlines for integration efforts are not likely to be met.
- When membership becomes more diverse after the working unit forms, communication challenges hinder trust-building, frustrate collaboration, and delay success.
- When agencies lack dedicated staff for community-level initiatives, program delays are likely to occur.
- When an interagency workgroup adapts its way of doing business to changing project realities, the group can execute more complex tasks.

These five lessons reinforce the 1997 observations of the National Defense Panel:

> Transformation will take dedication and commitment — and a willingness to put money, resources, and structure behind a process structured to foster change. Most of all, it will take wisdom to walk the delicate line between avoiding premature decisions and unintended "lock-in" with equipment purchases, operational concepts, and related systems whose effectiveness may erode precipitously in a rapidly changing conflict environment. (National Defense Panel, 1997, pp. 57-58)

Outlook: In this study, we found that badge interoperability is a complex system of systems. We believe that understanding how the many components of this system interact with each other will promote an understanding of how other IC systems operate, and that understanding will facilitate future efforts at IC collaboration and integration.

[2] Planned future phases will gradually expand the Intelligence Community Badge Interoperability Program to all other intelligence agencies.

The five lessons of badge interoperability — commitment, complexity, diversity, dedicated staff, and adaptability — provide insights to organizational culture and human behavior. These lessons have broad applicability to the security community (e.g., security clearance reform and master classification guide), and explain principles for any IC integration program.

Overview: The Director of Central Intelligence, the directors of the five agencies, and their security directors assigned responsibility for badge interoperability to a single security discipline (access control). They tasked a pre-existing group, the Access Control Working Group (ACWG), with program planning and implementation.

During implementation of Phase One, the ACWG members discovered that interoperability was more complex than expected. Executing the many tasks involved experts from multiple security disciplines, as well as experts in systems development, communications, and agency-specific requirements and processes. Bringing together these additional participants disrupted the established work patterns, which triggered communication challenges and even led to a few instances where one group of experts questioned others' motives.

This study identified examples of how one process or requirement can affect other agencies' processes and requirements. For example, one agency provided a server to another, but, because the two agencies had approved different software packages, the receiving agency had to execute a required software evaluation review process before it could use the server.

Despite interpersonal and technical challenges, the agencies worked together to develop creative, flexible solutions. By working and learning together, the agencies increased their mutual trust and demonstrated a true community perspective. Their success models for the rest of the Intelligence Community the benefits of persevering in joint projects.

The Five Lessons

This study of the 2003-2007 Phase One of the Intelligence Community Badge Interoperability Program (ICBIP) identified five lessons that are applicable to the specific case of upcoming phases of badge interoperability, as well as to broader integration efforts taking place in the Intelligence Community (IC). We will support these five lessons with insights drawn from two previous attempts to institute a common badge.

Apex was a 1970s' program for implementing a single security control system; a common badge was one of its planned projects. Badge reciprocity was an early- to mid-1990s' initiative that stopped at developing a standardized badge appearance that simplified facility entry for employees of participating agencies.

We organized our research design for this study around the following four questions:[3]

- What factors caused badge interoperability to succeed?
- In what ways did leaders at the Community and agency levels support and hinder badge interoperability?
- How did differences in agency culture affect badge interoperability (i.e., mission integration)?
- How does the Community assess its investments in information sharing and mission integration?[4]

The lessons we identified in this study reflect both the program's successes and "improvement areas," in the spirit of the *National Intelligence Strategy*.[5] Equipping leaders with these insights will help them make conscious decisions about what to repeat and what to do differently during future stages of badge interoperability and other IC integration efforts.

Lesson One — Commitment: When the Intelligence Community commits to addressing a well-defined need, success for an interagency program is more likely.

Intelligence Community personnel at all organizational levels exhibited strong commitment

Lesson: Being committed to task

Background: The IC's earlier attempts to promote badge interoperability failed. The pressures for information sharing after 9/11 demanded a mechanism for simpler employee visits and generated widespread commitment to interoperability.

Why it Mattered: When all levels of the IC were committed to badge interoperability, there was drive to complete the task in spite of obstacles.

---

3 For a detailed explanation of our research and analysis methodology, refer to Appendix A.

4 We collected data for this research question on investments, but the results did not yield a "lesson" as defined in our methodology. Most senior leaders and budget/finance officers thought the available financial data was not solid enough to provide a basis for such an assessment.

5 The *National Intelligence Strategy*, Enterprise Objective 9, states: "Learn from our successes and mistakes to anticipate and be ready for new challenges." "Mistakes" can have a negative connotation. We instead refer to "improvement areas" to promote a more positive perspective toward developmental growth.

to executing the first phase of badge interoperability. Earlier attempts to move toward badge interoperability were broader and unsuccessful. To demonstrate the power of commitment, we will compare the experiences of the 2003-2007 effort to the two earlier attempts — Apex and Badge Reciprocity.

Badge Interoperability — Phase One

Widespread support for badge interoperability came from senior leaders in the Community, the agencies, security offices, and from leaders at the working level. Senior-level direction — from the Director of Central Intelligence (DCI), Community Management Staff, and later the Director of National Intelligence (DNI) — compelled agencies to dedicate resources to interoperability.[6]

Just after the 9/11 attacks on the World Trade Center and the Pentagon, the global environment altered the IC mission to the point where existing visitor control practices were no longer viable. Both government and contractor employees visited other agency facilities more frequently. Because the badges in use were not interoperable between agencies, staff had to pass clearances and obtain visit certifications for many visits. Anecdotes depicted incidents when intelligence officers tried to enter other agencies' facilities during evenings and weekends, but could not get in because the offices that processed these types of visits were closed.

External pressures from Congress and the public forced the IC to consider considerable strategic and tactical changes to its business, but structural and cultural impediments made it easier to avoid the changes. In 2003, two years after 9/11, the IC had a clear problem around which it could rally.

The DCI issued the badge interoperability task in October 2003 during a period of significant Congressional oversight, the war in Iraq, and other global events. Agencies also faced staffing shortages stemming from the downsizing that occurred in the post-Cold War era (1990s). To meet the new demands, the agencies expanded their workforces and filled some formerly government positions with contractor employees.

Senior Leadership

Collective support from senior leaders, rather than leadership of any one individual, ensured program success. Senior leaders sustained their commitment to badge interoperability in spite of a lack of support by some audiences.[7] The Executive Director of Inter-Community Affairs (EXDIR/ICA) supported interoperability by directing the agency directors to realign resources

[6] Interviewees consistently attributed the interoperability tasking to the DCI; the issue of funding was less clear. Leaders at the working level interpreted the DCI's message of "do not worry about money" differently than those at senior levels. At the working level, many thought the DCI would provide extra funding for this mandate. Senior leaders thought that self-funding or a DCI tax was the typical, and appropriate, means to reallocate agency funds to Community priorities. The differing interpretations had no effect on execution, but did create a perception of unfairness for some agencies.

[7] Some agencies reportedly demonstrated their opposition by being slow to respond to requests, unwilling to explore alternative solutions to problems, and vocalizing opposition to the program.

to the program. The DCI Special Security Center (later renamed the DNI Special Security Center, or DSSC) funded a program manager position for coordination purposes. The deputy director of one agency reportedly made a personal promise to facilitate faster implementation.

Turnover among senior leaders did not affect support for badge interoperability. The Honorable Porter Goss replaced George Tenet as the DCI in September 2004. The Director of National Intelligence replaced the DCI position in April 2005, and the incumbent DNI changed in less than two years (February 2007). In addition, the directors of all five agencies and the security directors at four agencies changed. These new directors maintained funding and staffing support when they came on board.

Consistent leadership support for long-term reforms in the Intelligence Community is questionable, given career models that lead to regular turnover in the leadership ranks (Nagy, 2000). Political appointees may be tempted to focus on quick surface-level reforms, rather than time-consuming overhauls (Ostroff, 2006).

Support from career employees exerts a greater impetus for reform than support from senior leaders, especially political appointees. Career employees remain with their agencies longer than political appointees, so have a greater stake in long-term improvements. However, during their tenure, they may have witnessed many change efforts produce few results (Ostroff, 2006). Memories of unsuccessful reforms make some career employees skeptical of change initiatives.

The tiger team was motivated to see badge interoperability through to completion, despite the obstacles.[8] When the Community disbanded its central accreditation board[9] in the May 2006 timeframe,[10] the tiger team members nonetheless continued with the prerequisite work within their agencies.[11] Their diligence enabled them to obtain approval quickly, once the IC established a replacement board.[12]

---

[8] Some current tiger team members have been involved with the badge since badge reciprocity began. They said that interoperability was always the Community's desired goal, but was technically not feasible in the early 1990s. Because they have put forth so much energy toward this initiative, they were motivated to see interoperability through to completion. Regarding the belief that interoperability was not technically feasible in the 1990s, an interviewee said two agencies established limited badge interoperability — only 3,000 shared records — in the 1990s.

[9] The Defense and Intelligence Community Accreditation Support Team (DICAST) reviewed and approved accreditation packages for systems involving three or more agencies.

[10] We were unable to locate an exact cessation date for the DICAST. Intelligence Community Badge Interoperability Program (ICBIP) meeting minutes indicate that tiger team discussion about the issue began in May 2006.

[11] Each agency had to accredit its badge system before the Community could approve the full ICBIP system.

[12] The DNI Chief Information Officer (CIO) established the Intelligence Community Technology Governance Board, or ITGB, to be the accreditation authority for connections involving three or more agencies. The ITGB granted Interim Approval to Operate (IATO) for NSA, CIA, NGA, and NRO in December 2006, and to DIA in January 2007. With the IATO decision, the five agencies were permitted to share badge data on their live systems.

Lack of Commitment to Apex[13]

According to a source who attended Apex meetings with DCI Stansfield Turner, designing and implementing a common badge was an intended project under Apex.[14] The plan was to establish a common format similar to the format used with interoperability. An agency's security officer visually inspected the badge, and verified that the employee had a visitor certification.

The Community salvaged two projects planned for the cancelled Apex program — the 4C database (centralized clearance database) and the common badge. All participating agencies believed these initiatives would streamline security administration processes to their collective benefit, so they were interested. Little commitment was required because agencies dedicated few resources to implementing these two projects.

The Community did not develop a clear and compelling case to inspire the agencies...

Accounts suggest that the Community did not develop a clear and compelling case to inspire the agencies to welcome the changes Apex would bring.[15] Agency directors had full authority over their assigned intelligence disciplines. They had sole authority to manage the type of intelligence assigned to their agencies and explain the intelligence to senior policymakers. Little interagency analysis encouraged this parochial view.

Archival documents showed that the National Security Agency (NSA) asserted its responsibility to protect signals intelligence, which contradicts the intent of a single compartment under Apex. Oral history interviews documented industry's vocal opposition to the program.[16] Agencies circulated at least four alternatives to the implementation plan proposed by the Apex Steering Group. This showed the agencies' lack of commitment to the program.

President Ronald Reagan cancelled the Apex Program on 5 March 1981 (Leidenheimer, 1981). An interviewee attributed the program's failure to the change in presidential administrations. Others said simply that the Intelligence Community could not conceive of

[13] Because we did not find a complete history of Apex, we constructed a brief outline from archival documents and interviews. DCI Turner championed the Apex program as a replacement for the myriad agency-owned security control systems. Two interviewees thought President Jimmy Carter supported Apex to reduce the number of compartments and simplify work in the IC. *Aviation Week and Space Technology* (24 November 1980) characterized Apex as a system to stop the leaks of intelligence material. Two interviewees saw Apex as the DCI's initiative to centralize management of the Community under his control. These disparate viewpoints suggest widespread confusion about the goal of Apex.

[14] Recollections about the common badge in Apex were inconsistent. A member of the IC Classification Marking Implementation Working Group reflected in a 2008 e-mail that he believed the common badge was planned for Apex. However, we interviewed an employee who wrote one of the 1970s' Apex studies and did not recall that the common badge was part of Apex. White papers from the 1990s proposed the basic badge design and system architecture used for interoperability; these white papers do not reference Apex. Given the limited number of source documents available and amount of time elapsed, we prioritized the source who attended the meeting(s) with DCI Turner over the other sources.

[15] These accounts include original source documentation and interviews with people who had varying degrees of involvement in Apex. We also included insights from oral history interviews conducted in 1993 by an agency's office of security.

[16] This insight came from oral history interviews conducted in 1993 by an agency's office of security. These interviews were conducted for another purpose, and we did not validate the accuracy of past statements or their applicability to this study with the interviewees.

the possibilities and was not ready for it. We believe the lack of broad agency commitment, fueled by the IC culture and history, and the scope of the planned changes, caused its demise.

Commitment to Badge Reciprocity[17]

Badge reciprocity in the 1990s extended the common badge idea that began under Apex in the 1970s. Participating agencies accepted the common badge for facility access to their facilities, without requiring clearance information or a visit request. The agreements represented a shift toward interagency trust, at least for cleared government employees.

The procedural steps of passing clearance information to attend meetings required advanced planning, which reduced operational flexibility. Accounts suggest no strong organizational commitment to badge reciprocity.[18] However, implementation costs for badge reciprocity were so low that little organizational commitment was needed.[19] Additional intelligence agencies gradually signed on to badge reciprocity.

> ...implementation costs for badge reciprocity were so low that little organizational commitment was needed.

Lesson Two — Complexity: When full project complexities are not considered during initial planning, deadlines for integration efforts are not likely to be met.

All agencies expected to have technical complications with connecting their aging, disparate, and stand-alone badge systems. The tiger team members identified major program milestones and activities related to the technical aspects of the project. They broke the long-desired, monumental task of badge interoperability into achievable pieces, and estimated the implementation schedule. In addition, they developed creative solutions for unexpected technical challenges.

However, high-level technical planning did not account for the full extent of program complexities.

Lesson: Recognizing and overcoming complexity

Background: Unanticipated technical and process complexities made badge interoperability difficult to plan. Each additional agency introduced new details that further complicated this interagency program.

Why it Mattered: Unseen complexities are magnified in interagency program. These complexities negatively affect cost, schedule, and performance.

[17] Three agencies signed a Memorandum of Agreement to establish badge reciprocity between their facilities during the early 1990s. The agreements allowed government employees to visit participating agency facilities by presenting a common Community badge, without prior visitor certification. Security guards visually inspected the badge and assigned a Visitor/No Escort badge to the employee.

[18] These accounts came from individuals with varying degrees of involvement with badge reciprocity. We also used original source documents and oral history interviews conducted in 1993 by an agency's office of security.

[19] Assuming that posting protection officers at building entrances is required regardless of badge reciprocity, implementation costs were minimal. The agencies printed new badges and posters for each entrance that showed all approved badges. When describing badge reciprocity, one agency's security director called it a "low or no-cost solution."

Agencies needed longer than estimated to execute technical tasks. The unanticipated and unseen process complexities were not included in the high-level plan. Working through these complexities caused significant schedule delays. The DNI announced completion of Phase One approximately 17 months later than the published estimate.[20]

The tiger team did not produce a comprehensive planning document that showed all tasks and timelines for program implementation. The members opted to have individual agencies create and track their own schedules separately. Had a comprehensive plan been used, the tiger team would have to update it throughout the program, but the plan would have provided a central mechanism for coordinating activities across agencies.[21]

The technical and process complexities we will explain in this section made Phase One of badge interoperability difficult to plan and execute. We expect the complexities of implementing badge interoperability to increase exponentially as additional agencies join in future phases of the program.

Recognizing Program Complexity

Environmental and cultural factors complicated the program, but the agencies were unaware of these factors. Given a short deadline of six to nine months, the tiger team members believed there was insufficient time for planning. They anticipated the concrete milestones and developed basic cost and schedule estimates. They did not plan for process complexities because these complexities are embedded in the IC environment and culture and are invisible to the members of the IC.

Technical Complexities

Tiger team members expected to have difficulty connecting their agencies' disparate badge systems. Two badge technologies worked on different hardware. Software differences prevented the agencies from sharing their data directly. Until 2003, badge interoperability was limited to agencies using the same badge system.

The tiger team adopted a standard badge technology and anticipated some conversion costs. Two agencies upgraded their badge readers, motherboards, and related technologies to comply with the standard. The technical lead developed custom interface tables which translated data to enable the various systems to talk to each other.

When one agency re-classified its badge data after the initial Concept of Operations (CONOPS) was developed, another agency faced an unexpected hardware problem. Its badge system resided on a network with lower classification than the data being shared. The affected

[20] The tiger team published an estimate of 31 December 2005. We believe this date became an official deadline when the Executive Director of Inter Community Affairs (EXDIR/ICA) quoted this date in formal communications. On 20 April 2007, the DNI issued a Memorandum to the Intelligence Community announcing completion of Phase One.

[21] We initially focused on the omission of full project complexities from the initial planning. Upon further reflection, we determined this was a multi-faceted lesson that suggested areas to repeat as well as areas to improve. We share our progression to demonstrate the difficulty of recognizing project complexities.

agency considered its options before deciding to install a trusted agent.[22] Accrediting the trusted agent was an unanticipated task that added time to the implementation.

Sharing data across systems presented both expected and unexpected software challenges. The technical lead visited the agencies to see how their systems worked. The technical lead worked with each agency to identify the fields from which the data required for badge interoperability would come. This glimpse of functionality showed how each system processed its own data, but gave no indication of how each would process data coming from other agencies.

Differences in the agencies' data created some unexpected challenges. Three examples include the number of digits in one standard field, data format, and non-standard naming conventions.

Number of digits. The number of digits in the badge personal identification number, or PIN, was not standard. According to meeting minutes, the tiger team discussed this issue in detail. The agencies determined that changing the systems to a standard PIN length was not feasible. They came to a two-part resolution. First, the technical lead wrote a script that resolved the discrepancies. Then, the tiger team issued instructions to help badge holders enter the correct number of digits.

Format. One agency's system defined the social security number (SSN) as an "integer." This formatting dropped the initial digit of the SSN if it was a zero. As a result, some SSNs came through with eight digits, creating error messages at another agency.[23] The technical lead wrote a script to resolve the problem.

Nonstandard naming conventions. Tiger team members defined what information they would share, but did not specify standards, which introduced technical and process complexities to the program. For instance, agencies did not use the same format for names. Some included hyphens and apostrophes, but others did not. The tiger team agreed to accept incoming data as it was, but not all systems could support this decision, and they used technical and non-technical means to resolve the issues. Another agency installed a trusted agent that did not accept apostrophes; the technical lead wrote a script to remove apostrophes from data going to this agency. One system generated error messages when data did not match the record stored in its database. Badge office representatives called the other agencies to request corrections.

The issue of standard conventions for name fields exemplifies another type of complexity — process complexity.

Process Complexities

Process complexities, the intangible and often unseen elements of work, contributed to program delays. Conventions for the name data fields resulted in process complexities, as well as the technical complexities described above. In some agencies, the human resources (HR)

[22] Trusted agents are hardware installed between systems of different classification to prevent data spills. Some technical interviewees thought that accreditation for this trusted agent would provide a helpful precedent for other agencies in future phases of the program.

[23] One agency's system generates numerous error messages when incoming data does not match the expected format.

office or component owned the employees' name data and shared it with security. However, the standards for these fields were determined by the HR office or component, not security. Resolving the differences would require negotiations and unanimous approval of each security office, and each HR office or component.

We identified three types of process complexities that delayed badge interoperability: decision coordination, working across internal organizational boundaries, and unexpected processes.

Coordinating decisions. Coordination was required whenever decisions affected others' equities. Coordination within and across agencies served a useful purpose — it provided a mechanism "to ensure that everyone in the organization pulls in the same direction" (Mintzberg, 1994, p. 113). Tiger team members owned the responsibility to execute interoperability, but most of their decisions had to be coordinated. Although useful, coordination takes time, and this time was not built into the published implementation schedule.[24]

Even relatively simple decisions required buy-in from various parties or took extensive discussion to resolve. For example, badge printing became an issue when the Office of the Director of National Intelligence (ODNI) staff moved from CIA spaces to Bolling Air Force Base.[25] Meeting minutes show that the issue was discussed in May 2005, June 2005, and August 2005.[26] The agencies eventually reached agreement on printing the badges, although we did not find a specific record of the decision.[27]

Stovepipe issues.[28] Many badge interoperability tasks went beyond the purview of security. Therefore, coordination across agency boundaries was required. A senior leader called these complexities "stovepipe issues." While badge interoperability was among the highest priorities for security, it appeared not to have the same priority for those outside of security. For example, two agencies reported some extensive waiting periods to receive communications support.[29] One agency said it successfully used its relationships to pre-coordinate firewall support with the appropriate team, and did not experience this type of delay for its firewall.

Several tiger team members were frustrated with stovepipe issues related to accreditation

---

[24] The tiger team established a schedule with the 31 December 2005 deadline, but with a caveat that provided timely approvals and accreditations.

[25] The issue about badge printing may have resulted from the appropriations process. Congress approves funds for designated activities. We think that printing DNI badges may not have been included in either CIA or DIA appropriations.

[26] When asked about decisionmaking, several interviewees mentioned the difficulty of settling the badge printing situation. The dates referenced in this paragraph come from ICBIP Tiger Team meeting minutes.

[27] The end decision was for CIA and DIA to share responsibility for printing, depending on where the staff member was assigned. The Defense Intelligence Agency (DIA) prints all badges except for employees who spend more than 50 percent of their time at CIA. In those cases, CIA prints the badges. We did not find a reference to the actual decision.

[28] Stovepipe issues are challenges caused by organizational structure in which separate but equal management chains are established; no manager has control over another manager's operation, and they make informal agreements within established relationships to facilitate work tasks.

[29] Communications support included such tasks as installation of a fiber optics line, or communication drops.

(ACWG, 2006b). The DSSC program manager recognized that the tiger team had no control over most tasks. Therefore, the program manager asked whether the tiger team members tried to influence others to expedite required tasks. Some members appeared reluctant to get assistance from senior leaders to resolve the issue.

Unknown sub-processes. Agencies review hardware and software for security risks and maintain a list of pre-approved products. To use an alternative, the requestor must submit the product for security review and obtain a waiver. The IC did not have a single, standard approved hardware and software list, which created an issue when the technical lead agency gave a server pre-loaded with a database to another agency. The two agencies approved different databases, so the receiving agency sent the database through the required review before using the server.[30] This review time was not built into the published schedule.

Planning for Complexity

In *Harvard Business Review,* Mintzberg (1994, p. 110) wrote, "Work processes must be fully understood before they can be formally programmed." Because most of the process complexities were not recognized or fully examined, program planners could not be expected to accurately estimate schedules.

The tiger team did not produce a comprehensive, interagency planning document for the program.[31] Some participants believe, in retrospect, that a complex plan would not have helped because there was a lack of precedent, and they made a large number of course corrections during Phase One. Participants in a complex operation involving several intelligence and law enforcement agencies expressed a similar view about advance planning (CIA, 2007).[32]

Anticipating problems and planning for contingencies formalized the steps to take so that agencies could implement them "almost automatically" (Mintzberg, 1994, p. 108). When they prepared cost estimates for the Required Order of Magnitude, agencies included technical staff members to varying degrees. Program complexities played a significant role in cost. Some interviewees did not believe the complexities could have been anticipated because ICBIP was the first program of its kind. In contrast, other interviewees believed that experience in access control did not prepare the tiger team members to anticipate these technical and process complexities.[33]

---

[30] A tiger team member called the review process "an extra hoop to jump through." This sentiment is common outside of security, and may offer an outreach opportunity for encouraging support for security functions.

[31] Meeting minutes show that in August 2006, a tiger team member requested a comprehensive plan that showed all agencies' tasks and dependencies up to implementation. During the discussion, members mentioned that a plan was used earlier in the program, but they found that individual agency plans were needed.

[32] We believe advance planning is critical in situations where lives are at risk. However, the potential consequences of discovery-based or ad hoc planning for badge interoperability were not life-threatening.

[33] Technical interviewees from two agencies said ICBIP was the first accreditation package they had worked on. The accreditation processes were not routinely enforced before 2003, but the basic requirements were not new. Employees with a background in information systems security might have more experience with these requirements than employees with access control backgrounds.

Historic Lessons about Complexity

The Apex program was designed to provide special protection for information that warranted it, and enable maximum dissemination of intelligence product while protecting sources and methods (National Foreign Intelligence Program Working Group on Compartmentation, 1979).[34] An interviewee who served on an Apex working group said the IC convened at least a half-dozen work groups to study and/or plan Apex. The scope of Apex grew to encompass multiple security processes, such as access control. Another interviewee, who attended Apex meetings with DCI Turner, said the IC planned to design and implement a common badge.[35]

The greatest lesson of Apex comes in examining its process complexities. The DCI proposed significant changes to the Community. Two interviewees described the demise of Apex as the IC's being "not ready for it." Coordinating draft studies gave agencies opportunities to express, and possibly strengthen, their opposition to Apex. Survival of a planned technology initiative (the 4C database) suggests that non-technical issues played a primary role in Apex cancellation.

Lesson Three — Diversity and Trust: When membership becomes more diverse after the working unit forms, communication challenges hinder trust building, frustrate collaboration, and delay success.

Lesson: Adjusting to diversity

Background: Initial planners formed mutual trust through years of joint experience. New people and new expertise altered the team's composition and dynamics.

Why it Mattered: Interdisciplinary conflicts degraded trust and collaboration.

Organizations frequently define *diversity* as differences resulting from personal background (i.e., nationality, race, or sex). We adopted a broader definition of diversity: variety in knowledge, skills, and experience. The mix of security, communications, and technical expertise made badge interoperability possible, but also created communication challenges that degraded relationships.

Conflicts between agencies masked disagreements between disciplines — i.e., between technical staff and tiger team members.[36] While individual tiger team and technical staff

[34] During a 1993 oral history interview, a retired security officer said the Apex objectives were to provide better protection to the most sensitive information, and make the information readily available to the military.

[35] Another interviewee did not recall that Apex included a common badge. White papers from the 1990s do not reference Apex. Given the limited number of source documents and amount of time elapsed, we prioritized the first-hand source over the other sources.

[36] Both technical staff and tiger team interviewees reported incidents that caused them to question the other group's intent and competence. Individually these incidents look like interagency disputes. Viewed as a whole, however, these incidents suggest a pattern of mistrust between the two implementation groups. For instance, some wondered what the technical lead was saying about their agencies during senior leadership meetings; it turns out the technical lead went to meetings to explain technical details. Interviews revealed significant internal conflicts between technical team and tiger team representatives at one agency. Turnover of technical managers caused disruption for the implementation team; in contrast, turnover among tiger team members did not produce the same level of disruption. We believe the role of the technical manager played a larger role in implementation success than that of the tiger team representatives.

members worked together before interoperability, the implementation team as a whole was a brand new entity. Tiger team members planned most of the program and tapped their technical counterparts to varying degrees. Each agency completed most technical tasks alone, giving the technical implementers few opportunities to work through problems together. In addition, tiger team and technical staff members were unfamiliar with each other's areas of expertise, precluding them from making full use of each other. The two groups did not trust each other, which limited the success of the collaboration.

Team Diversity and Trust

Homogeneity of the Access Control Working Group (ACWG)[37] gave members a deep understanding of the same concepts, terminology, and issues. Their jobs involved access control issues such as badge issuance and visitor control, and this shared background facilitated joint discussion and problem solving. Research suggests that team members collaborate more easily and naturally if they perceive themselves as being alike (Gratton and Erickson, 2007). Group norms, such as introducing one's successor, provided orderly transitions that further fostered relationships. The members' homogeneity and relationship building gave the tiger team a natural foundation on which to start badge interoperability.

Team makeup must include the right sets of skills and knowledge. However, disparities in skill and knowledge "spark insight and innovation" but can hinder collaboration (Gratton and Erickson, 2007, p. 102). Building the right team may necessitate bringing together individuals who do not get along "nicely," which contradicts the "default mode" of some organizations (Fischer and Boynton, 2007, p. 118).

Because they did not have much experience working together, the tiger team and technical experts in hardware, software, communications, and other disciplines gradually forged their mutual trust.[38] When new technical staff joined the program, they sometimes questioned established plans, sparking tensions with some tiger team members. These questions derived from the technical staff's familiarity with terms, concepts, and process issues unfamiliar to the tiger team. In addition, some of the technical experts were contractors. Limits to direct interaction between contractors introduced new challenges to team dynamics.

Little Trust

Regular meetings over a long period of time helped tiger team members develop a high degree of familiarity and deep mutual trust. This trust eased the tiger team members'

[37] The badge offices from several Intelligence Community agencies formed the Access Control Working Group (ACWG) in 1993 to establish badge reciprocity and move toward a Community-wide badge. Tiger team refers to a sub-group of the ACWG that planned and implemented Phase One of badge interoperability. When the IC badge interoperability program began in 2003, the homogeneous membership of the tiger team included only badge office representatives who were government employees.

[38] One agency realized enough benefit from technical participation in the tiger team meetings that it chose to have the technical representatives represent this agency on the standing ACWG, instead of the non-technical security officer.

potential discomfort of asking for help in front of their peers. They felt assured that their ideas and concerns would be considered during decisionmaking. Technical staff members, on the other hand, had fewer opportunities to interact with their counterparts in other agencies. Their diverse expertise and limited mutual trust failed to produce this same level of comfort and assurance.

Technical staff said they did not have an interagency forum dedicated to technical issues. Some technical interviewees believed they could have solved some problems more quickly if they had discussed technical issues together, instead of figuring them out alone. On the other hand, tiger team members and some technical staff questioned the benefit of such a forum. From their perspective, the technical staff could not give meaningful assistance to other agencies because their badge systems were significantly different.[39]

According to tiger team members, technical staff did not take advantage of all the available opportunities for interaction. For example, the technical staff did not always attend "Technical Exchange Meetings,"[40] which were open to all interested parties. Technical staff typically attended only the meetings targeted for their agencies.[41]

Agencies executed most technical tasks either unilaterally or bilaterally (i.e., without significant interagency collaboration between all five agencies). Agencies upgraded their infrastructures and obtained accreditations with little involvement of other agencies. They worked bilaterally with the technical lead to design interface tables, and configure firewalls and public key infrastructure (PKI)[42] certificates. The technical lead appeared to work alone on developing the interface tables and developing scripts to resolve small technical issues.

Agencies executed most technical tasks for badge interoperability unilaterally or bilaterally (i.e., without significant interagency collaboration)...

Many technical staff members were contractors. As a result, they had limited freedom to communicate directly with their other agency counterparts. Whether the limitations were real or perceived, most of the contractors believe they had to route communications through a

39 Technical staff members had different specialties, but understood many of the same terms, requirements, and development processes. Because they had some shared background, we believe they were equipped to be a greater help to each other.

40 The technical lead held Technical Exchange Meetings (TEMs) at each agency to discuss technical details and issues.

41 A government manager wanted to minimize contractor time spent in meetings. This manager said tiger team meetings focused only on administrative issues, so sending contractors to all meetings was too expensive. However, the manager did not mention whether this concern applied to TEMs.

42 Public Key Infrastructure, or PKI, refers to a form of encryption that keeps information from being decrypted by anyone except the recipient who owns the corresponding private key. The Intellipedia article on PKI (as of 7 August 2008) offered an analogy to explain PKI: a locked mailbox with a mail slot. The article says: "The mail slot is exposed and accessible to the public; its location (the street address) is in essence the public key. Anyone knowing the street address can go to the door and drop a written message through the slot; however, only the person who possesses the key can open the mailbox and read the message" (Public Key Infrastructure, Intellipedia, 2008).

[government] manager.[43] Message relays created multiple opportunities for misunderstanding and delay, which fueled distrust.[44]

Interaction Contributes to Successful Transformation

In addition to achieving project objectives, satisfaction with project interactions is an element of collaboration success (Vlaar, Van den Bosch, and Volberda, 2007). The agencies met the project objective by completing badge interoperability. They were less successful on the second element of collaboration success — generating participant satisfaction with their interactions.[45] Tiger team members and technical staff disagreed on the necessity of rapport between technical staff.[46] Internal agency dynamics between technical staff and tiger team members created communication difficulties that sometimes directly affected other agencies.

Multiple opportunities for direct interaction give people a chance to create new meaning out of information, which alters perceptions and makes possible changes in behavior and practice (O'Neill and Jabri, 2007). Receiving the badge interoperability task triggered several agencies' defensive routines. According to several senior security leaders and tiger team interviewees, some initial reactions included:

- "[Badge interoperability] breaks too many policies"
- "We need the right people to do this"
- "We need more systems engineering"
- "[*This* agency] is never going to go along with this"
- "It's too hard"
- "[The technical team] almost laughed us out of the room"

Regular interactions between tiger team members reviewed all technical requirements and capabilities, and listened to each agency's concerns. The group made a series of decisions that satisfied the needs of each agency, and made all representatives satisfied with the process and the end result.

Despite success with tiger team planning and interaction, agencies executed most of their technical tasks unilaterally or bilaterally, giving few opportunities for technical staff to resolve their differences. In addition, working unilaterally and bilaterally limited the opportunities for

---

[43] We were confused by two contradictory ideas regarding communications. Tiger team members said they needed to know all program details so they could make decisions and keep the senior leaders informed. On the other hand, they also said that technical staff members knew "when to pick up the phone." These ideas were expressed during two "roundtable" meetings we held to give the tiger team opportunities to validate data and initial findings.

[44] Several technical interviewees were frustrated at relaying information through non-technical managers; technical staff members believed their questions were not adequately conveyed or addressed. An e-mail between two tiger team interviewees suggested that they, too, were frustrated. However, they continued to relay information throughout Phase One.

[45] Satisfaction with the interactive process makes the participants want to participate again in the future. We believe that increasing satisfaction will encourage agencies to collaborate and share information.

[46] In response to a technical staff member's comment that "we needed rapport with [*the technical lead agency*]," a tiger team member from a third agency said, "We didn't need rapport. We just needed to share data."

trust to build between the technical staff and tiger team members. An outcome of continued separation and little trust, both technical and non-technical members interpreted each other's behavior negatively, reducing their satisfaction and overall program success (Vlaar, Van den Bosch, and Volberda, 2007).[47]

For example, technical interviewees questioned other agencies' security standards and requirements. Agencies had different requirements for system testing and backup.[48] One interviewee believed that the technical lead's suggested firewall would provide insufficient security for his/her agency's data. Some technical interviewees thought their concerns were ignored by the non-technical managers. Interviewees (technical staff and a tiger team member) said the technical lead was slow to respond to questions. We heard, but did not see any supporting documents for, claims of data tampering by the technical lead agency.

This lack of trust in other agencies' knowledge and competence hint at five issues the Information Sharing Environment Program Manager (ISE-PM) described in a preliminary report on establishing the Information Sharing Environment. The Community Interoperability and Information Sharing Office (CIISO) report quoted the ISE-PM preliminary data as follows:

> ...organizations do not fully trust one another when sharing information... there is widespread concern that other users of the disseminating agency's information may not have the necessary skills, training, and knowledge to interpret and use it properly...a key goal of any information sharing training plan must be to change IC culture in this area. (CIISO, 2005)[49]

Interagency Trust in Comparison Cases

Apex triggered cultural issues such as data ownership and whether employees were equally trustworthy. Security practices at the time protected information by strictly limiting access to it. These protections reflected agency-centric perspectives, which held that agencies owned *their* data, rather than that the U.S. Government owned the data. The common badge violated the security practices of the time, but did not generate the level of opposition that other aspects of Apex generated.

Reciprocity started small, with three agencies signing a memorandum of agreement, and later expanded to more intelligence agencies. The agreements defined the business rules for granting reciprocity to government employees, and the agencies specifically excluded

[47] Some interviewees privately shared their perception that the technical lead imposed standards on the other agencies.

[48] Requiring duplicate systems or connections gives the agency a place to run tests without harming live systems, and provides a backup in the event of system failure. Agencies with less stringent requirements spend less money, but openly accept more risk.

[49] Tiger team members questioned the applicability of the CISSO report to badge interoperability. They attributed the lack of trust in the other firewall to the agency's desire to continue using products with which their firewall team(s) were familiar. They also thought the agencies wanted to avoid changing their existing contracts with the vendors.

contractors (NSA, 2003). Agencies realized only marginal cost savings because reciprocity procedures relied on traditional "visitor" badging activities (NSA, 1995).

Changes to classification management practices lessened the cultural concerns of trust and integration before badge interoperability happened.[50] Despite their concerns about cover issues and contractors, the agencies adopted procedures that facilitated interagency visits. Simultaneous growth of the IC and reductions in budget caused agencies to reduce the strict system of compartmentation from the days of Apex.[51]

Lesson Four — Using Dedicated Staff: When agencies lack dedicated staff for community-level initiatives, program delays are likely to occur.

Lesson: Using Dedicated Staff

Background: Managers assigned Community tasks as additional duties. In juggling assignments, employees lacked the time or attention to persuade the chain of command to assist when schedules were in jeopardy.

Why it Mattered: The additional duties can burden staff and cause delays.

The Intelligence Community Badge Interoperability Program started as a DCI mandate with a short deadline; the agencies did not receive dedicated funding for execution. The time required for one of the agencies to recruit an extra person would have exceeded the initial program deadline. Managers faced a decision to increase the workload of key players, temporarily suspend regular duties, reassign duties to another person, or adopt some combination of these solutions (Sirkin, Keenan, and Jackson, 2005).

Workload and Staffing

...workload during a change initiative should not increase by more than 10 percent...

Research suggests that workload during a change initiative should not increase by more than 10 percent, to avoid taxing resources such that either the change program or normal operation is compromised (Sirkin, Keenan, and Jackson, 2005). Badge interoperability added new responsibilities and new subject matter to the workloads of tiger team members and technical staff. Everyone juggled interoperability with their ongoing assignments. Some employees supported temporary duty assignments during interoperability.

Agencies used some workers temporarily "to carry out routine activities or to outsource current processes" (Sirkin, Keenan, and Jackson, 2005, p. 113). A senior leader reportedly

[50] The Community was reclassifying information to the lowest level possible in order to enable greater dissemination but still protect sources and methods. Agencies had, or were considering, moving much of their compartmented data to the SI and TK compartments. Both compartments are included in the baseline access for Top Secret//Secret Compartmented Information.

[51] Clearance reciprocity was a major factor in encouraging interagency relations. Agencies recognized other agencies' clearances, provided there were no eligibility concerns. Polygraphs complicate the picture, even with badge interoperability. Some agencies require a full scope polygraph, while others require a counterintelligence (CI) scope polygraph for access to information systems. Full scope polygraphs are fully accepted by all agencies, but CI scope polygraphs are accepted only by some agencies.

reassigned an employee to assist with interoperability temporarily until a replacement team member arrived.[52] Another agency tapped a staff member who was between assignments to print their badges.

According to Heifetz and Laurie (2001), "managers may consider [transformation] work a priority, but have difficulty sacrificing their familiar ways of doing business" (p. 136). At the DNI level, agency taxes and self-funding demonstrate familiar methods of funding joint activities. Another familiar method of meeting priorities is to postpone assignments; agencies only said they postponed activities — they did not specify which ones.

Process complexities added to the burden of these additional duties. Tiger team members had to navigate their agencies' internal organizational structures and processes to get tasks finished. For instance, they navigated chains of command to make inquiries and requests for assistance. They notified the right leadership of decisions before executing them. Security-relevant changes involved even more coordination between directorates/offices.

Effects of Other Duties

Intra-agency and interagency coordination takes time and attention. Senior leaders reported that pre-coordination and developing relationships helped ease "stovepipe" issues in badge interoperability. Internal coordination between directorates was a challenge, especially for two agencies that required installation or support for communications lines. For instance, communications reportedly told security that a new connection was active, but not where it was installed. Agencies reported mixed results in getting support for firewalls.

Senior leaders reported that pre-coordination and developing relationships helped ease internal "stovepipe" issues in badge interoperability.

Time and individual personality played a role–some at the working level appeared reluctant at times to work the chain of command to obtain the necessary support.[53]

Communication between the tiger team and technical teams had varying degrees of quality. Some technical staff and a tiger team member reported slow response times to their questions and requests for assistance. These interviewees said the technical lead did not respond to their questions sufficiently or within a reasonable period of time. They also reported making multiple phone calls and sending multiple e-mails before receiving a response. In one instance, the technical staff member reportedly "gave up" because his agency was tired of waiting for a response and needed to move forward.

Since the tiger team was not dedicated to this single program, their ability to handle coordination efforts effectively suffered, contributing to a prolonged implementation schedule.

[52] According to interviews with a senior leader and a technical staff member.

[53] We did not see evidence that leaders withheld any requested support. However, the data suggests that some working-level leaders were reluctant to seek management support outside security.

Dedicated Staff in Comparison Cases

The degree to which an additional duty differs from the employee's regular job and experience affects the success of the additional duty model. Programs may be considered simple if they fall within one person's purview. Program execution may be simple if the employee has experience in the particular topic or function. Asking employees to perform regular duties while gaining expertise in entirely new functions or topics creates a demand that surpasses the recommended maximum 10 percent increase in workload (Sirkin, Keenan, and Jackson, 2005).

Agencies detailed staff members to approximately six working groups that conducted studies and wrote the implementation plan for Apex.[54] The task force model may have contributed to the completion of the planned studies. In this case, the agencies were required to provide resources to the Apex program, but they had no organizational commitment to full implementation.

In its study on Apex, the working group of the National Foreign Intelligence Program (NFIP) recommended that "the shortfall in positions and associated funds be underwritten by the participating members of Apex. This would avoid the need for the full burden to be absorbed by the DCI and "reinforce the communal nature of the program" (NFIP, pp. 29-30).

Agencies did not create extra positions or dedicate new resources for badge reciprocity. However, reciprocity did not significantly change or increase staff duties. During reciprocity, representatives of the badge offices continued to work within the access control domain. In contrast, interoperability drew access control offices into information systems development, and certification and accreditation, among other subject matter outside the tiger team members' areas of expertise.

Lesson Five — Adaptability: When an interagency workgroup adapts its way of doing business to changing project realities, the group can execute more complex tasks.

The tiger team's ability to adapt to program changes was critical to successful execution of this complex program. Interoperability involved more detailed planning and a greater degree of agency interdependence than previous efforts. As it encountered problems, the tiger team evaluated its options, and figured out how to proceed (Katzenbach and Smith, 2005).

Lesson: Adapting as individuals and groups

Background: The working group members were undeterred by the program issues that arose. Members successfully leveraged their program history to solve problems and build a foundation for future success.

Why it Mattered: Effective group process and personal resilience ensure long term group success.

According to two individuals who spent much of their careers in the IC, the durability of the larger ACWG is highly unusual (MS&O, 1993). The group built on established, trusted relationships and work processes. The Phase One agencies formed a sub-group of the standing

[54] This insight came from oral history interviews conducted in 1993 by an agency's office of security.

ACWG to focus on badge interoperability. They met weekly at first and with decreasing frequency as the program progressed. The ACWG practice was to note deliberation points and decisions in meeting minutes; the sub-group adopted this practice, which facilitated their group success.

Elements of Successful Collaboration

Two elements of performance apply to interagency collaborative efforts: achievement of goals and satisfaction with the interactions (Vlaar, Van den Bosch, and Volberda, 2007). In this case, the agencies achieved their shared goal. The badge symbolized IC integration, and satisfaction with the process to execute interoperability could spur additional cross-agency integration.

Two elements of performance apply to interagency collaborative efforts: achievement of goals and satisfaction with the interactions.

The agencies completed most program tasks individually, but kept each other informed of their progress. They did depend on each other for ultimate success — the IC could not really say it executed badge interoperability if one of the big five agencies was excluded.

Formal coordination and control mechanisms set expectations that enable satisfaction among group members (Vlaar, Van den Bosch, and Volberda, 2007). Tiger team members adapted existing agreements instead of starting over whenever needs changed. Mutual expectations for funding and duties were included in the Interconnection Security Agreements. They also circulated and approved meeting minutes to ensure that the formal record of group deliberations and decisions was accurate.

Tiger team members used meetings to define, re-define, and make sense of various aspects of the Intelligence Community Badge Interoperability Program (ICBIP). This conversation-based learning helped ICBIP maintain its momentum in the face of multiple changes in senior leadership in the Intelligence Community (O'Neill and Jabri, 2007). Members worked more closely than they did before ICBIP. However, they lacked structured discussion and decisionmaking processes, which prolonged debates about some issues.

The ICBIP Memorandum of Agreement defines the agencies' areas of responsibility, but it does not specify group processes (Bardach, 2005). Groups use charters and detailed ground rules to determine, in advance of the need, procedures for considering issues and new ideas, how much time to allow for debate, and steps for decisionmaking. For example, the team talked repeatedly about the proper placement of the badge magnetic strip. Most tiger team members were satisfied with the discussion processes and wanted to continue similar interactions.[55] However, the technical team members did not share this satisfaction with the extended debates.

[55] Tiger team members were satisfied with the length, content, and outcome of their debates. However, some members thought certain debates continued for too long. One interviewee said, "We discussed everything to death."

Integration of New Members

Tiger team members set up group processes for status reporting; these processes helped ensure the agencies' participation and satisfaction. In January 2005, the DCI Special Security Center (DSSC) issued a quarterly report template for reporting on program status to senior agency and community leaders (ACWG, 2005). The template provided a stoplight chart (green/yellow/red) format to report status in four areas: hardware integration, software integration, system testing, and re-badging. The template also provided space to report significant issues and/or changes. The technical lead agency later altered the template to provide information that better represented milestones and the work they were performing.

The team demonstrated a level of flexibility that saved the agencies time and money and kept the tiger team viable for future phases. The members re-used existing program documentation when program changes occurred. For instance, agencies added annual financial requirements to the Interconnection Security Agreements (ISAs) between each agency and the technical lead, which helped them work with their budget offices to plan for annual expenses and future recapitalization.

To integrate new members, the team provided copies of detailed meeting minutes, stoplight charts, and other documentation. The documents conveyed program history, as well as *the way things are done.* Groups often do not talk about *the way things are done* until a new person violates an organization's deep-seated value or norm. Knowing little things, such as the group's way of introducing successors or that issues and problems are openly discussed, facilitates the new member's integration to the work group.[56]

Overcoming Obstacles

The Director of National Intelligence, established after badge interoperability started, created some uncertainty for the tiger team. When the DNI formed the Intelligence Community Chief Information Office (IC CIO) in 2006, the IC dissolved the Defense and Intelligence Community Accreditation Support Team (DICAST), which was the accrediting body for systems involving three or more agencies.[57]

To implement badge interoperability, the agencies needed DICAST approval. The tiger team kept working through the period of uncertainty because its members recognized the DICAST issue was actually irrelevant. Before they could request DICAST approval, each badge system first had to be accredited by its own agency. The tiger team pursued the agency accreditations, and a replacement board was established in time to approve the badge interoperability program.

[56] Program history and cultural orientation were not given to all technical managers when they became responsible for ICBIP tasks. This omission contributed to the diversity-related communication challenges mentioned in an earlier lesson.

[57] The DICAST was the accrediting authority at the beginning of the ICBIP; it was dissolved in 2006 after the Office of the Director of National Intelligence (DNI) was established. The DICAST was re-formed under the IC Chief Information Officer (IC CIO) as the Intelligence Community Information Technology and Governance Board (ITGB). The ITGB granted Interim Approval to Operation (IATO) to the ICBIP on 19 December 2006. The IATO allowed the agencies to begin sharing badge data on their live systems. In effect, IATO gave the agencies permission to roll badge interoperability out to the population.

The tiger team demonstrated its flexibility and perseverance when it gained concurrence for a common badge design.[58] When an agency wanted to add a seal to the back of the badge, the tiger team members did not immediately say "no." The tiger team referred to the ICBIP Concept of Operations and discovered no prohibitions against it. Eventually the agencies agreed to set aside a part of the back of the badge for the agencies' discretionary use.[59]

Turnover among government personnel (technical and tiger team) necessitated, but also tested, the implementers' adaptability. Badge office representatives changed for three of the five participating agencies. More disruptive were changes of technical managers at two agencies. Long-serving members of the group said that every time a new member came on board, they had to explain the program concepts and architecture again. A collective belief emerged that past decisions could not be revisited because the agencies had already traveled so far down an implementation path.

Adaptability in History

Agencies were assigned authority to manage certain types of collection. These authorities gave agencies license to assume ownership of the data they collected. This provincial desire to protect *their* information or equities grew out of data ownership. Given this background, the agencies' resistance to most forms of standardization or centralization is understandable.

Interviewees with varying degrees of involvement with Apex said that program managers established their own security procedures. Leaving decisions to individual prerogative resulted in great disparities between programs — not to mention between agencies. Workers maneuvered intricate security procedures. They sometimes went through multiple background investigations to work programs for a single agency. Some individuals believed that agency leaders must personally be expert in the disciplines they manage. They view efforts at central management, whether by the DCI, CMS, or DNI, as micromanagement.

After President Reagan cancelled Apex in 1981, the Community decided to salvage two planned projects. The Community-wide, Computer-assisted, and Compartmented Control System, also known as 4C, was a government-wide database of clearances and accesses.[60] The 4C system contained data on cleared persons from approximately 16 agencies. Each agency was responsible for keeping its own data current. Most updates required manual entry, although one agency reportedly automated its updates. Agencies fell behind, and, as the data became increasingly outdated, they stopped using 4C.[61]

---

[58] The Community Badge was designed to be identical on the front side of the badge. Some security officers interpreted the agreements as requiring agency badges to have identical front and back designs. Others thought changes to the back were acceptable. Instead of advocating their respective positions, the tiger team referred to source documentation for guidance, and quickly decided to concur with the request.

[59] We did not find a specific record of this decision.

[60] One interviewee provided an alternate explanation for the name 4C. At the time of the Apex program, the NRO was a classified organization housed at the Pentagon in Room [redacted] According to this interviewee, 4C came from the room number. (b)(3)

[61] We derived this statement from two interviews: a personal interview with a security officer who used 4C, and an oral history interview conducted in 1993 by an agency's office of security.

Establishing badge reciprocity demonstrated adaptability. Security officers stretched their thinking to consider the possibilities and implications of reciprocity. They evolved their past business processes to allow government employees to visit other agencies without a visit certification.[62]

[62] Some long-serving government employees in the IC said they were required to pass their clearances before visiting other agencies, even after badge reciprocity was in place. We verified with a tiger team member that under reciprocity, government employees were not required to do so. Even though badge interoperability has been in use for over one year, implementation challenges remain. For example, in Spring 2008, Senior Intelligence Service employees registering for an interagency training course were asked to pass their clearances, even though they carried the fully interoperable IC badge.

The History of Success — Phase One Badge Interoperability (2003–2007)

In October 2003, the Director of Central Intelligence (DCI), George Tenet, tasked CIA Security and the DCI Special Security Center (DSSC) to find out how much time and funding would be needed to establish an interoperable community badge.[63] This push to create an interoperable badge for the IC — an initiative that had been attempted twice before, with Apex in the 1970s and Badge Reciprocity in the 1990s — proved to be successful because the post-9/11 geopolitical environment was more conducive to implementation.

Along with representatives of the "Big Five" agencies (CIA, DIA, NGA, NRO, and NSA), the Directors of CIA Security and the DSSC considered alternatives such as buying a new, common badge system, or making software changes.[64] In November 2003, the Big Five agencies developed a plan that would enable the five disparate, stand-alone badge systems to share data, with eventual replacement of the badge systems (i.e., in approximately six years).[65]

The security directors transferred responsibility for badge implementation to the Access Control Working Group, or ACWG.[66] In December 2003, the representatives of the Big Five formed a subgroup of the ACWG to work on implementing the Intelligence Community Badge Interoperability Program (ICBIP); this team is known in this report as the "tiger team."

Program Planning and Management

In point of fact, ICBIP was not a "program" in the strict sense of the word, with one senior official commenting that the word "Program" in ICBIP was a misnomer. There was no central program office, budget, or authority, and no one manager was the overall decisionmaker for ICBIP. Differences in program and management terminology caused confusion and contributed to delays in execution.

Moreover, among tiger team members there seems to have been a lack of clarity about who exactly was the program manager. In interviews, they gave conflicting answers when they were

[63] We did not find formal documentation from these early events. This account is based on several interviews, including interviews with the two senior security leaders who received the tasking directly from the DCI. Appendix B contains a chronology from Phase One of badge interoperability.

[64] The director of one agency reportedly threw his collection of IC badges on the table during a senior leadership offsite and demanded to have one badge that worked everywhere. This anecdote is often repeated, but neither in the documents we found nor in the oral history interviews we conducted — to include officers who participated in the meeting — were we able to find corroboration to prove that this dramatic incident actually happened.

[65] There was little agreement about the intended implementation plan. Two senior security leaders said the agencies planned to make software changes as a short-term solution until agencies could plan for a long-term recapitalization. In other words, they planned to buy a common badge system for all agencies later. In contrast, some tiger team members expected future phases of badge interoperability to continue with the software changes made during Phase One.

[66] Representatives of intelligence agency badge offices formed the ACWG in 1993 when a small number of intelligence agencies began considering badge reciprocity. Members met regularly, even after the initial badge reciprocity agreements were signed, to work other access control and security issues and to pave the way for future badge interoperability.

asked to identify the ICBIP program manager; most said the technical lead agency was the program manager.[67] One explanation for this lack of clarity may be that badge interoperability started in 2003 as a short-term project to be executed from existing resources, rather than a formal program or major system acquisition.

Two entities held the title "program manager" during Phase One. When the DCI told the agencies to execute badge interoperability in October 2003, a participating agency volunteered to be the executive agent.[68] The DNI Special Security Center assigned a program manager for ICBIP in approximately November or December 2003.[69] When the new program manager was named, the executive agent became the "technical lead." None of the program documents we reviewed distinguished the technical lead's role from the program manager's role.

To make sense of the confusion, we examined the functions of a program manager. The DNI provides this working definition of a program manager:

> ... [the] position and...individual accountable for cost, schedule, and performance of [a major system acquisition or project] and typically responsible for the management of conceptualization, initiation, design, development, test, contracting...to satisfy IC elements' needs, intended for use in, or in support of, intelligence missions. (ODNI, 2008a)

The program manager from the DSSC was accountable to the security directors for interoperability status and progress, but lacked the authority and resulting influence to ensure that agencies adjusted their resources and activities to meet the established schedule. The technical lead had in-depth knowledge of the badge systems, so a representative of the technical lead reportedly attended meetings to support the program manager on technical questions.[70]

The DSSC program manager assumed some coordination duties from the technical lead. He convened regular tiger team meetings and circulated a formal record of their discussions. He encouraged tiger team members to work through their respective chains of command to address task delays, but this encouragement was not always sufficient. Workload and personality of individual tiger team members affected their effectiveness with escalating program issues.[71] In addition, the program manager became a self-described "mediator," resolving issues when the tiger team could not come to consensus on its own.

---

67 The DSSC manager entered the position after ICBIP started and lacked knowledge of program history and concepts. Because the technical lead had this background, most tiger team interviewees thought the technical lead was better equipped to manage the program. This view continued until the end of Phase One, even though the DSSC manager understood the background of the program.

68 Although the other agencies accepted the executive agent's offer to take on additional responsibilities for the program, other agencies appeared to resent the arrangement over time.

69 We were unable to determine from interviews and source documents the reason why the DSSC waited to assign a program manager, nor could we determine the date the program manager assumed this position.

70 One aspect to the confusion is that some believed attendance at the security director meetings was a managerial role. A representative of the technical lead clarified during a tiger team meeting that the technical lead attended those meetings in a supporting role as backup to the program manager.

71 We did not see evidence that leaders withheld any requested support. However, the data suggests that some working-level leaders were reluctant to seek management support outside security.

In some respects, the technical lead assumed roles typically performed by the program manager. The technical lead reportedly guided other agencies through the technical aspects of badge interoperability.[72] The technical lead better understood the technical details, and was, therefore, better equipped to relay status information throughout Phase One. The technical lead assisted the program manager by answering technical questions during meetings with the security directors.

Some events support an alternative view that no one functioned as the ICBIP program manager. Regardless of who held the title "program manager," Intelligence Community customs dictate that all decisions be coordinated with the right parties. This custom is especially true when a decision crosses agency boundaries. For the ICBIP, no one person directs resources or changes schedules.

The tiger team did not produce or maintain a comprehensive plan that showed all tasks that each agency was completing. They preferred to track their own agencies' tasks separately from the other agencies.[73] There was little advanced planning or established problem solving approaches to help the agencies address issues. Tiger team members instead followed a discovery-based approach to program execution, figuring out solutions after problems occurred.[74]

The tiger team members together drafted cost estimates for the Rough Order of Magnitude (ROM), first submitted in February 2004.[75] They updated the cost and schedule figures as new program details emerged. In July 2004, they established 31 December 2005 as the implementation deadline.[76] Tiger team interviewees from four agencies said they never believed this deadline was reasonable, but still supported it.[77]

Tiger team members interpreted the DCI's message "not to worry about funding" differently than the security directors did. Because badge interoperability was mandated by the DCI, the tiger team believed the DCI (and later DNI) would fully fund ICBIP.[78] Having more experience with interagency programs, senior leaders believed that the agencies would

---

72 Source: Interview with a tiger team member.

73 Tiger team meeting minutes suggest that an early comprehensive plan was discontinued in favor of individual agency plans.

74 Some tiger team and technical interviewees said the technical challenges they overcame could not have been foreseen, so a comprehensive plan would not have been helpful. Interviewees familiar with technical development projects in the Intelligence Community said it was normal for technical challenges to come up only after implementation, and that certain challenges could never be anticipated. A technical developer who works outside the IC agreed that every development project includes unanticipated challenges, but said these project schedules typically build in time to identify and resolve these challenges.

75 The initial ROM was dated 21 January 2004.

76 IC Badge Interoperability Program Timeline, dated 20 July 2004 (see Appendix C).

77 During a roundtable session, tiger team members reported that they communicated *acceptable* deadlines. They believed that the agency leaders would not accept longer timelines, even though the short deadline was arbitrary. One security director reported asking why the schedule kept being delayed and asked implementation team members for a "real" schedule that they could meet.

78 Program documents show a meeting on 21 January 2004 in which the tiger team developed initial cost estimates. The team revised the ROM estimates as they discovered additional program details.

fund ICBIP, either through a DCI tax or self-funding.[79]

The Intelligence Community Badge Interoperability Program (ICBIP) started as a DCI mandate with a short deadline; the agencies did not receive dedicated funding for execution. One agency said the time needed to recruit, hire, and orient an extra person was longer than the announced program schedule.[80]

Tiger team members considered the options: increase workload of key players, temporarily suspend regular duties, reassign duties to others, or select a combination of these options (Sirkin, Keenan, and Jackson, 2005). All of the agencies asked staff to juggle interoperability and their ongoing assignments. In many cases, members of the tiger team were forced to learn brand new subject matter.

Agencies had limited control over their staffing. A senior leader reportedly reassigned an employee from a different critical job to assist with interoperability until a replacement team member arrived.[81] Another agency brought in a staff member who was in between assignments to assist with badge printing; this temporary arrangement did not require additional funding.[82]

System Design and Execution

Tiger team members were responsible for implementing badge interoperability, but they relied upon various technical and communications teams to execute the tasks. Because the technical staff in some agencies reported to managers outside security, tiger team members had difficulty expediting tasks.

The ICBIP consists of servers that translate outgoing data from agency-unique formats into a standard format, and incoming data back into a format the individual badge system can read. This "translate and send" concept builds on a technique two agencies used to share badge data in the 1998 timeframe. The technical lead learned about each system's data fields and functionality, and then developed custom database tables that performed these translations.[83]

The technical lead constructed a system architecture that would enable existing badge systems to send and receive data over a Virtual Private Network, or VPN. A VPN is a private connection, or tunnel, through which data is sent over a public network. The technical lead used Public Key Infrastructure (PKI) to encrypt the tunnels so that only the intended recipient

[79] Tax refers to a required transfer of funds between agencies. Self-funding refers to agencies reallocating their resources to fund implementation. In this case, the DCI (through the Community Management Staff, or CMS), directed agencies to provide funds for shared interoperability costs. Later communications instructed agencies to reallocate resources to implement badge interoperability.

[80] Interviews with a tiger team member and a technical staff member.

[81] Source: Interviews with a senior leader, tiger team member, and a technical staff member.

[82] Source: Interview with a tiger team member.

[83] Building the translation tables provoked an interagency conflict, and possibly competition between contractor companies. One agency's manufacturer required the technical lead to sign a special nondisclosure agreement before the manufacturer would share information such as data fields and format. The government had legitimate concerns about protecting the company's proprietary information, so the agreement was reviewed by the Office of General Counsel, and select representatives of the technical lead agency signed the agreement. According to tiger team members, this was a simple misunderstanding — no proprietary information was ever requested.

(i.e., other agencies participating in ICBIP) could read it.[84] The ICBIP was among the first Intelligence Community programs to utilize the tunnel concept on a live system, a major success for the participating agencies.

The technical lead identified the encryption standards for the system and suggested a firewall for the other agencies to use. These firewalls allow only approved users to view data, and only approved data to pass through. Each agency was free to choose any firewall that was compatible with the encryption standards.[85] Each agency connected to the technical lead's system and adjusted their encryption and system settings until everything functioned properly.

Without dedicated funding for additional staff, the technical lead agency added badge interoperability to the workload for its contractors and specifically postponed select projects and maintenance activities.[86] The contractor juggled multiple assignments, and worked separately with each agency on ICBIP tasks, such as configuring firewalls, establishing connections, building data interface tables (for translation from one system format to another), and troubleshooting. Mission needs dictated that this contractor employee complete periodic temporary duty assignments during Phase One. Tiger team and technical interviewees from two agencies said the technical lead's support contractor was unresponsive at times, in part due to heavy workload.[87]

Although the tiger team members were responsible for ensuring the success of badge interoperability, technical staff members were responsible for execution. Differences in organizational structure affected the way certain staff worked together (i.e., who could be involved in a communication, or who could approve something). The technical staff in some agencies reported to offices or directorates outside security.

Setting Standards

The tiger team established the minimum common standards required for participating in ICBIP, and agencies determined for themselves how to meet the standards. Besides such standards as badge technology, communications, and encryption, the tiger team identified what data the agencies would share. Program scope issues (e.g., whether the DCI intended to include contractors) came up early and were not fully resolved until the end of Phase One.

---

[84] Public Key Infrastructure, or PKI, refers to a form of encryption that prevents all except the intended recipient, who holds the right private key, from decrypting the information. The *Intellipedia* article on PKI (as of August 7, 2008) explained PKI with this analogy: a locked mailbox with a mail slot. The article says, "The mail slot is exposed and accessible to the public; its location (the street address) is in essence the public key. Anyone knowing the street address can go to the door and drop a written message through the slot; however, only the person who possesses the key can open the mailbox and read the message." (Public Key Infrastructure, *Intellipedia*, 2008.)

[85] A technical interviewee said that firewalls used to be manufactured in such a way that they were incompatible with firewalls developed by other manufacturers. Over time the firewalls have become more standard. The agencies adjusted their firewall settings to connect them properly.

[86] Source: Interviews with representatives of the technical lead agency.

[87] We believe that the original work plan placed a heavy burden on the technical lead agency, and contributed to Lesson Four (Using Additional Staff). One agency shouldered a heavy portion of work for this Community initiative. It may have created a perception of unfairness that in the future could degrade interagency relationships. Unsuccessful collaboration would almost certainly reduce agencies' willingness to support future Community-wide initiatives.

The tiger team compared two badge technologies in use at the participating agencies before they selected a standard. They cited two reasons for choosing the selected technology standard: a majority (three out of five agencies) used it, and the selected technology was more current and included more unique identifiers.[88] Unless the other two agencies made extensive upgrades to firmware,[89] badge readers, and related equipment, they would be unable to participate in badge interoperability. The tiger team members also determined the data they would share[90] and the basic standards for their data fields.[91]

Early debates on program standards, and, in one case, the extended time required for resolving a dispute, suggest that agencies were not accustomed to compromise or interagency collaboration.

Culture and Politics

Badge design discussions throughout Phase One centered on format and mechanics, but reflected the challenge of uniting the agencies under cohesive leadership and merging their distinct cultures. Some of the contentious issues that emerged during Phase One of ICBIP included extending participation in the Community badge program to U.S. Congress intelligence staff members, whether interoperability should extend to contractors, and even the standards for badge design and card stock features.

Changes in scope. In June 2006, the Undersecretary for Defense Intelligence (USDI) announced the Congressional staff badge, known in security as "the purple badge" (Tiger Team, 2006). Tiger team members believed the purple badge inappropriately extended an IC badge to Congressional staff members, who are part of the legislative branch of government, not the executive branch. Some security officers said that Congressional staff members are not always subject to the same vetting as members of the IC.

Including the purple badge in Phase One would have introduced extensive changes and delayed the program further. After learning of the potential delays, the senior IC leaders in August 2006 approved a temporary compromise: introduce the badge for visual validation and entry, but postpone interoperability. The agencies established acceptable business rules that assured some level of control, but simplified facility entry for Congressional staff and did not require system changes.[92]

Contractor participation. Contractor participation in ICBIP was among the first issues

---

[88] Unique identifiers are pieces of data in a database that apply to a single record. For example, an agency might use unique identifiers to verify the identity of a badge holder.

[89] A technical interviewee described firmware as custom code that enables the motherboard to read data. In this case, the firmware upgraded motherboards to enable the badge readers to read the standard badge technology.

[90] One agency was concerned about protecting the cover of certain employees. Its representatives were concerned that sharing identity information would create security issues. This agency decided on a solution that would protect the cover of these employees.

[91] Two interviewees said that commercial off-the-shelf (COTS) systems do not provide all of the information needed to perform access control in the IC. Although considered to be COTS, IC badge systems are customized. The lesson of complexity suggests that, if the agencies continue to use the "translate and send concept," technical and process errors will multiply as more agencies join ICBIP.

[92] Derived from interviews with tiger team members and e-mails about the event.

to be raised, and among the last to be resolved.[93] Agencies always disagreed on whether the DCI intended badge interoperability to include contractors. Some worried that contractors would use their IC badges to enter other agencies for "marketing purposes." Some interviewees believed that contractors cannot be trusted to use their badges for official purposes only.[94]

With one exception, agencies with a longer history of interagency missions or larger contractor populations tended to support contractor inclusion.[95] The DNI Special Security Center instructed the agencies to include all contractors in March 2007, approximately one month before the DNI declared completion of Phase One.[96]

Changing the badge. Interagency debates resurfaced whenever an agency proposed even small changes to its badge. The tiger team reserved a small square on the back of the badge for agencies' discretionary use.[97] Requests to tailor this reserved section were generally supported after some discussion.

For instance, in November 2005, two agencies planned to add special notations in the reserved section (e.g., a logo, and "SES" notation for senior level staff). Tiger team members pondered the potential "trickle down" effect of these badge modifications, and some believed these changes would negate the April 2005 counterintelligence assessment of the badge.[98] They ultimately supported the agencies' decisions to tailor the reserved section of the badge.

On the other hand, the tiger team actively opposed requests to change the front of the badge. In May 2005, one agency planned to add a background flag to the pictures on senior executive and flag officer badges; this request was not supported or implemented.[99]

Badge stock. The selected badges had a magnetic strip on back; determining whether the strip belongs on the left or the right turned into a contentious issue. The technical lead ordered the initial set of badge card stock in October 2004. Ten months later (August 2005), the technical lead re-opened the debate after a new technical manager asked about standards and insisted on using COTS material. Agencies stated and restated their positions. These extended discussions were moot; not only could badges be ordered with the magnetic strip on either side,

---

93 According to meeting minutes and several interviewees, the DNI Special Security Center instructed the agencies to include all contractors in March 2007, approximately one month before the DNI declared Phase One to be complete.

94 Official purposes include any mission or job requirement validated by the government. A non-official visit might involve visiting another agency's facilities to see their buildings, without having a legitimate job-related need. Minutes from several tiger team meetings show repeated discussions about the issue.

95 Source: Interviews with tiger team members and a senior security leader.

96 Source: Interviews with senior security leaders and tiger team members.

97 This agency-specific section of the badge is noted in the ICBIP Concept of Operations. We did not find a specific record of the decision to allow agencies to customize this section of the badge.

98 In April 2005, counterintelligence representatives and security directors reviewed the badge from a counterintelligence perspective. They found that the badge would provide updates and audit capabilities that enhance security.

99 We believe that this instance of interagency debate demonstrated the cultural challenge of integrating agencies that value rank differently.

the agencies were already moving toward other technologies.[100]

Several agencies said no existing commercial access control system provides the full data necessary to bring someone into their facilities. Badge offices pull additional information on the badge holder from systems owned by human resources or other entities. Each system has varying ability to handle data variations, such as hyphenated names or apostrophes. The tiger team decided not to standardize the format of data fields during Phase One, instead directing agencies to accept data exactly the way it came in.[101] However, one agency's system was not programmed to support this agreement. It generated lengthy error reports, and at times overwrote the badge holder personal identification numbers (PINs).

All agencies needed to have a firewall to protect their data on its way to other agencies. The technical lead, with tiger team input, set encryption standards for the firewalls. They suggested a product, but agencies were free to select their own firewalls. According to tiger team members, agencies selected the contractors with whom they already had established contracting mechanisms and with which their technical staff was knowledgeable. A technical staff member believed the firewall suggested by the technical lead provided inadequate security for "this agency's" data. This competing view reflects the lack of interagency trust and diversity issues, which are explained in the findings section of the paper.

Accrediting Systems

When badge interoperability began, DCI Directive (DCID) 6/3 required agency systems to undergo the certification and accreditation process.[102] In this two-part process, agencies documented their systems' functions and known security risks, and formally accepted, or accredited, the risks. DCID 6/3 prescribed certification and accreditation (C&A) milestones, but each agency could autonomously establish its own procedures. Accreditation lasted for three years, or until a security-relevant change occurred.[103] The difficulty of obtaining accreditation increased along with the system risks.[104] Each badge system had to

[100] Two tiger team members and three technical interviewees described extended debates on placement of the magnetic strip. These two groups held opposing views of the discussions. Tiger team members believed this type of discussion is a healthy part of working together. One tiger team member attributed the disagreements on the magnetic strip to one new technical manager's personality. Technical interviewees, on the other hand, believed the tiger team preferred to discuss administrative issues rather than hard, technical issues.

[101] Meeting minutes and interviews show consensus on this agreement, but we did not find a specific record of the decision.

[102] Intelligence Community Directive (ICD) 503 (Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation), signed on 15 September 2008, supersedes DCID 6/3. This study describes the DCID 6/3 requirements because these were in effect throughout Phase One of badge interoperability.

[103] According to DCID 6/3, a security-relevant change is any change that affects the system's functionality or risk.

[104] The difficulty of obtaining system accreditation relates to the system's Protection Level (PL). Agencies set PL based on the system user's clearance, access, and need to know. If all users have these elements for all of the system's data, it is a low-risk system with a low PL. Countermeasures are needed to address the additional risks of systems with higher PL. Documenting the risks and countermeasures can add significant time to the accreditation process.

be accredited, but so did the overall ICBIP system. Tiger team members called accreditation "the long pole in the tent."[105]

While subject to the same basic requirements, intelligence agencies interpret and implement these requirements differently. No one person knew the full pathways for all five accreditation processes, complicating program management. One agency's stringent requirements for testing and backup caused it to install an extra test connection to the technical lead agency.[106] Alternatively, one agency reported that it had to arrange periods of downtime for system maintenance and testing.

One agency's actual business practices (i.e., the steps it followed to update and upgrade its badge system) ran contrary to its documented certification and accreditation process. Interviewees said that the technical staff customized the badge system upon request. However, most of these changes were executed without the formal documentation, approval, or testing required by DCID 6/3 and agency directives. The changes built up over time to the point where the system functionality differed significantly from what the manufacturer expected. After upgrading to a new version and installing patches, the agency's badge system crashed in March 2005. The technical manager and team toiled under stressful conditions to restore functionality, and continued for several months to obtain accreditation.

Some implementers had little experience with managing complex technical projects, which may have contributed to program delays.[107] For example, technical interviewees from two agencies said that working with ICBIP was their first experience with accreditation. These interviewees learned how to develop the required documentation by attending training and on-the-job discovery. The agencies faced another type of challenge resulting from inexperience with technical projects: when certain requirements are not met during accreditation, additional processes apply. The five Phase One agencies did not anticipate this type of requirement.

For example, the technical lead decided to provide a server to another agency during the Fall of 2005. This server contained a database product that was not on the recipient's approved list. On 8 February 2006, the receiving agency explained to the rest of the tiger team that a waiver for the database was necessary because of the approved software list.[108] This extra review contributed to the receiving agency's schedule delays.

---

[105] Derived from context, "long pole" means that the duration of the program grows in accordance with the duration of the accreditation process. That is, faster accreditation leads to faster ICBIP implementation.

[106] An interviewee from a different agency questioned the rationale for this duplicate connection, suggesting that the requirement was too stringent.

[107] During a roundtable meeting, tiger team members disagreed with the view that experience played a role in accreditation challenges. An alternative explanation was that no one could have anticipated these program challenges.

[108] Agencies maintained their own lists of approved hardware and software. If they wanted to use products that did not appear on the list, they were required to submit the product for an extra security review process. If the risks were deemed acceptable, the agency's designated security representative issued a waiver to allow it to use the new product. Agencies can only accredit systems that use approved products, regardless of the process followed to obtain this approval.

Interviewees disagreed on the adequacy of ICBIP test plans. Agencies divided responsibilities for installing, testing, and maintaining parts of the ICBIP connection and documented them in their Interconnection Security Agreements. Each agency unilaterally developed test plans for its own areas of responsibility, without approval or guidance from the technical lead. The technical lead wrote a high-level plan to cover the full ICBIP, but wrote detailed test plans only for its areas of responsibility. A technical interviewee believed that the technical lead was supposed to approve the test plan, but went ahead with the testing without the technical lead's approval when he or she did not receive timely feedback.[109]

Turnover, especially among technical managers, contributed to accreditation challenges. New team members reviewed and questioned the CONOPS and other program plans. Other members explained program plans each time the agencies changed representatives. Some tiger team interviewees thought it was too late to revisit program plans because program implementation had already started.

The IC Grants Interim Approval to Operate

The tiger team briefed the Defense Intelligence Community Accreditation and Standards Team (DICAST)[110] on the ICBIP concept and architecture at least two times. The fate of ICBIP became uncertain in 2006 when the new DNI formed the Intelligence Community Chief Information Office (IC CIO) and disbanded the DICAST. Throughout these changes, the tiger team repeatedly discussed the uncertainty and continued to pursue accreditation within each agency.

Once the IC CIO was functioning, it established the new Intelligence Community Information Technology Governance Board (ITGB) to fill the void left by DICAST dissolution. The five participating agencies submitted the following documentation for final review.[111]

- Interconnection Security Agreements (finalized and signed between September-October 2006)[112]
- Test procedures and plans with documented results
- Each Agency's Approval to Operate (ATO) for their access control systems

The ITGB reviewed the documentation and granted interim approval to operate (IATO) on the following dates:

- 19 December 2006: NSA, CIA, NGA, and NRO
- 17 January 2007: DIA[113]

---

[109] We do not think the technical lead was responsible for approving other agencies' test plans. The DICAST/ITGB was the Community-level accreditation board responsible for connections involving three or more agencies. DCID 6/3 assigned responsibility for approving and executing test plans to the entity responsible for the system. Therefore, we believe the responsibility to approve the end-to-end test plan belonged to the DICAST/ITGB.

[110] The DICAST was the accrediting authority for all systems that connected three or more agencies.

[111] ITGB replaced the former DICAST as the central community body with purview over systems that connect three or more agencies.

[112] Source: ACWG Meeting Minutes and copies of signed Interconnection Security Agreements.

[113] DIA's accreditation was issued separately from the others because its accreditation package was not ready at the same time as the other agencies' packages. (Source: DIA interviewee)

As a result of the IATO, the five agencies could share live badge data through ICBIP. Tiger team members said they conducted two visits to each agency to test their badges. The agencies tweaked their systems to resolve errors, and gradually opened up the system to all employees.

Program Success

The DNI announced successful completion of Phase One of badge interoperability on 20 April 2007 (McConnell, 2007). The tiger team and technical representatives together forged new ground for the IC. The ICBIP was among the first live IC systems to establish encrypted tunnels over a VPN, with validation by PKI certificate.[114] The five agencies triumphed over non-technical process complexities to make the long-desired goal of interoperability a reality.

Senior leader interviewees believed that ICBIP was the right investment not for financial reasons, but because it furthered the Community's integration and information sharing goals. Agencies tracked certain program costs, but were unable to trace hidden costs such as staffing as an "additional duty."[115] Therefore, without knowing the full costs, they did not believe they could make a full evaluation of the investment.

Today, members at all levels of the Intelligence Community swap success stories about getting into other agencies' facilities. Although currently limited to a few agencies, the IC Badge Interoperability Program has made a significant contribution to IC integration and information sharing.[116]

[114] Tiger team and technical interviewees said badge interoperability was among the first applications of tunneling implemented in the IC. The PKI certificates added identity validation to the system, making it more secure.

[115] One question asked during early stages of the study was, "Does badge interoperability save money?" Several tiger team interviewees believed that it would reduce waiting times for visitors and the number of administrative staff needed for processing visitors, and, therefore, generate cost savings. (Some of these ideas were proposed in earlier white papers on the common badge.) Senior leaders and budget officers estimated the high technical and infrastructure costs to be greater than the resulting administrative efficiencies. Many factors interact and hidden costs cannot easily be tracked, causing us to conclude that further research into this question is unwarranted at this time.

[116] There are limited situations where a person may have two or more badges. Some agencies require anyone using their information systems to hold a badge issued by that agency. For instance, a contractor who supports contracts at two agencies may receive badges from both agencies. Some non-security personnel were slightly disappointed that the ICBIP did not completely eliminate multiple badges. Despite their disappointment, all appreciated the simpler visitor procedures.

Two Earlier Attempts — Common Badge (1970s) and Badge Reciprocity (1990s)

Long-serving intelligence community officers reported that administrative security processes were cumbersome in the 1970s and 1980s. Interviewees described the procedures they followed to visit other intelligence agencies. Security offices validated clearances against data sources, and entered visitor certifications to a local system. Upon arrival, the security office representative verified the visitor's identity and issued a local badge for entry. Each simple step added processing time, but did not necessarily improve security. A former analyst from the CIA Directorate of Intelligence said these visit procedures discouraged her from working with other IC analysts.

Some in the IC believe the badge interoperability program was a post-9/11 innovation that started in 2003. We discovered that the U.S. Government previously tried two times to implement a standard community badge. Apex was a 1970s' attempt to simplify security compartmentation and administration through such improvements as a common badge. Badge reciprocity was a more successful 1990s' initiative under which agencies established written agreements that simplified entry for employees of participating agencies.

At the beginning of this study, some tiger team members said they believed badge interoperability was impossible before 2003 because technology was unable to support it. It appears that the decentralized structure and history of the IC was a more important factor inhibiting interoperability. Congress and the public demanded that the IC collaborate and share information to a greater degree after 9/11. Badge interoperability became a way for the IC to demonstrate concrete progress toward these qualitative ideals.

We did not find complete histories for the earlier attempts to establish a single IC badge. This brief history of these earlier attempts comes from our review of source documents in agency archives and interviews with employees who had varying degrees of involvement with these earlier attempts.

Apex: First Effort to Institute a Common Badge (1979-1981)

President Jimmy Carter came into office during a period of unprecedented criticism and oversight of the Intelligence Community (IC). The Director of Central Intelligence (DCI) during much of Carter's tenure, Admiral Stansfield Turner, established Apex to resolve the security structures and processes that were widely perceived as impediments to work. Several accounts suggest that Apex was designed years ahead of its time.

Rationale for Apex (Early 1970s)

During the early 1970s, exposure of CIA activities by the press led to a period of unprecedented criticism and oversight. These revelations fueled public mistrust and calls for reform in the Intelligence Community. Throughout the presidency of Richard Nixon, revelations of CIA involvement with assassinations and other illegal activities caused a "public outcry" (Turner,

2005, p. 24). *The New York Times* published excerpts of the Pentagon Papers, which revealed secret details about the Vietnam War in June 1971 and damaged the public's view of the government in general (Weiner, 2007, p. 318).

In 1971, Nixon directed James Schlesinger to conduct a three-month study of the roles and responsibilities of the DCI. Schlesinger's review found "the cost of intelligence was soaring and the quality shrinking... [and] there is no evidence that the intelligence community, given its present structure, will come to grips with this class of problems" (Warner and McDonald, p. 21). According to former CIA historians Michael Warner and J. Kenneth McDonald, the Schlesinger Report recommended a "strong dose of management" with greater centralization (Warner and McDonald, 2005, p. 22).[117]

The Watergate scandal stoked the mistrust of government. Nixon resigned in the wake of Watergate and President Gerald Ford came into office on 8 August 1974. President Ford continued the strong oversight of the Intelligence Community. According to a former CIA historian, President Ford established the Rockefeller Commission to investigate CIA activities after *The New York Times* wrote a story about domestic spying. The Senate also set up an investigation panel (the Church Commission), as did the House of Representatives (known as the Pike Commission). The Church and Pike Commissions made serious inquiry into the CIA and the IC, and prompted external calls for reform (Haines, 1999).

Senior government leaders expanded their investigations to include other previously sacrosanct activities. In 1975, the United Stated Intelligence Board (USIB) Security Committee chartered a task force to examine compartmentation and recommend ways to ensure "timely and full utilization of intelligence products" (USIB, 1975, p. 1). The task force concluded that agencies frequently overclassified their information, and recommended changes that would increase product dissemination but still protect the most sensitive programs and projects (USIB, 1975).[118]

Jimmy Carter assumed the Presidency in January 1977, and he tried throughout his presidency to expand the powers of the DCI.[119] He appointed Adm. Stansfield Turner (USN, Ret.) as DCI. Soon after Carter's inauguration, Congress formed two panels to provide oversight to the IC — the Senate Select Committee on Intelligence (SSCI) in 1977, and the House Permanent Select Committee on Intelligence (HPSCI) in 1978 (Turner, 2005, p. 24). Until these committees were established, the IC was subject to little external management and accountability.

Demands to simplify security controls grew in 1978, after an interagency working group sponsored by Turner found that agencies "jealously guarded" access to their information (DCI

---

[117] James R. Schlesinger, Assistant Director, Office of Management and Budget, "A review of the Intelligence Community," 10 March 1971, as cited in Warner, Michael and McDonald, J. Kenneth, *"U.S. Intelligence Community Reform Studies Since 1947,"* Center for the Study of Intelligence, Washington D.C., April 2005, pp. 21-22.

[118] Internal working copy comments about the draft *United States Intelligence Board (USIB) Security Committee Task Force Report on Compartmentation*. 22 December 1975.

[119] Oral history interview with Stansfield Turner, former DCI, 18 July 2000 (Interviewer unidentified).

Working Group on Compartmentation and Codewords, 1978, p. 3). This working group found that agencies protected a growing number of projects in compartmented systems, and that the protection assigned for sources and methods was "often inconsistent with their true sensitivities" (DCI Working Group on Compartmentation and Codewords, 1978, p. 2). In other words, agencies overclassified their data.

The Apex Program[120]

Turner planned to reorganize the entire Sensitive Compartmented Information (SCI) community under DCI authority.[121] This shift would enhance the DCI's ability to simplify security in the IC. Turner convened the National Foreign Intelligence Program (NFIP) Working Group on Compartmentation to develop the Apex security control system, which had three objectives:

- Replace the several systems for compartmented intelligence with a single, Community-wide system
- Develop a system that permits maximum dissemination while protecting sources and methods
- Define which intelligence "clearly warrants special protection" (NFIP, 1979, p. 1)

Clearing employees to the Apex compartment would make them eligible for access to most IC information. The implementation plan defined standard criteria for protecting the most sensitive information under Apex sub-compartments protected under the code name Royal.[122] A small number of people whose jobs required access to the sensitive operational details would be cleared into the appropriate sub-compartments. The working group planned to strictly limit the number of people cleared into these sub-compartments.

Multiple groups planned the detailed implementation steps for Apex.[123] One group defined criteria for assigning information to sub-compartments, and another group designed cover sheets.[124] Agencies estimated costs stemming from Apex, such as updating software or traveling to provide indoctrination briefings to all employees.[125] Estimating the resources needed to implement Apex was reportedly difficult because the "anticipated procedures... [were] not

[120] The program name, Apex, is not an acronym or an abbreviation. Apex refers to the single control system under which all intelligence information would fit.

[121] Sources: One interviewee not directly involved with Apex but who worked in the Sensitive Compartmented Information (SCI) community at the time, and a 1993 oral history interview of a retired security officer.

[122] Royal was the codeword designated for the compartmented system within Apex. As with the name Apex, Royal is not an acronym or abbreviation.

[123] Memorandum for the National Foreign Intelligence Community from the Chair of the National Foreign Intelligence Board, dated 27 October 1978, p. 2; and two interviewees with varying degrees of involvement with Apex.

[124] During an office of security oral history interview (1993), a retired officer described Apex program objectives differently, in a way that resembles the post-Gulf War and post-9/11 emphasis on making intelligence products readily available to the military.

[125] Oral history interview conducted in 1993 by an agency's office of security, and a current interviewee who was directly involved with Apex.

known to the degree and at the level necessary" (Inman, 1980, p. 1).

The Working Group on Compartmentation anticipated that implementing Apex would "permit the consolidation of the security policy and administrative functions" (NFIP, 1979, p. 25). A source who attended Apex meetings with DCI Turner said the agencies planned to design and implement a common badge for the IC.[126] The common badge established a foundation for badge reciprocity in the 1990s and badge interoperability in 2003.

The working group's goal was to reduce the processing required for interagency visits by cleared government employees. The common badge would serve as validation of the holder's identity and clearance. Before an agency would grant entry to the badge holder, he or she needed a visitor certification.

President Jimmy Carter approved Apex on 8 January 1980. He signed Presidential Directive/ NSC-55, which stated that Apex would provide uniform security standards for "access to, distribution of, and protection of sources and methods (The White House, 1980, p. 1)."

Apex Unravels

Unaccustomed to the level of suspicion and investigation that occurred during the early 1970s, the IC resisted demands for change. Apex tested their fundamental security philosophies, and agencies perceived it as a challenge to their authorities and missions. Agency leaders were accustomed to operating autonomously and unilaterally. Each agency believed it had sole control over the data it collected. For instance, a former government employee believed that Apex would have removed flexibility and malleability in applying the control system owned by his agency and would have eliminated the autonomy his former agency needed.[127]

Agencies loathed the idea of relinquishing power over *their* control systems. Each agency had authority over a full system or parts of a system. For instance, NSA owned the Comint control system, and the National Reconnaissance Office owned the Byeman control system.[128] An interviewee experienced in security policy and classification reported that different agencies owned information protected under the Talent-Keyhole control system.

Parochial interests led government program managers to establish their own security processes, resulting in little consistency across programs, much less across agencies.[129] Apex represented a paradigm shift toward standardization and openness in the IC. Another explanation for Apex's collapse was DCI Turner's leadership failure to inspire the agencies to

[126] A different interviewee, who contributed to an Apex study, did not recall that the program included a common badge. White papers from the 1990s, which propose badge interoperability concepts, describe the basic badge format in use in 2008. These white papers do not reference Apex. However, given the limited source documentation and amount of time that has elapsed, we prioritized the source who attended the meeting(s) with DCI Turner over the other source.

[127] Oral history interview conducted in 1993 by an agency's office of security.

[128] The NRO retired the Byeman Control System on 22 May 2005.

[129] Oral history interview conducted in 1993 by an agency's office of security.

accept it.[130]

The IC did not fully understand the goals of Apex. Interviewees said Turner championed Apex as a simplification of the security control systems in the Community. *Aviation Week and Space Technology* (24 November 1980) characterized Apex as a system to stop the leaks of intelligence material, which were reportedly common in the 1970s. Two interviewees viewed Apex as the DCI's scheme to take control of the Community. Government and industry perceptions held that senior leaders were trying to "ramrod" Apex, and representatives of these two groups resented the interference from the DCI.[131]

Another contributing factor to Apex's demise was that the intelligence agencies did not trust Turner. The widespread resistance to Apex described earlier in this section suggests that agencies disliked oversight in general, not just that provided by Turner. On the other hand, agency employees perceived him as a so-called "outsider" because Turner never served as an intelligence officer. In addition, current and former CIA employees shared their personal beliefs that Turner damaged CIA's capabilities because he downsized many positions.[132]

Apex challenged the basic premise of a security control system. Protecting information by limiting the number of people who have access to it was the cornerstone of security practices since the IC's inception. The guiding philosophy for IC security and business practices was the need-to-know concept.[133] This deeply ingrained concept kept IC employees from comprehending how Apex could work. On the other hand, agencies voluntarily degraded the importance of need-to-know by increasing the number of people who were cleared, to the point where the processing became "unmanageable" (NFIB, 1978).

Turner also failed to resolve interagency differences, especially those between defense and intelligence agencies. Each agency maintained its own authorities, and cited lack of dedicated funding as a reason not to implement Apex.[134] For instance, NSA thought agencies did not agree on what constitutes "a proper SCI briefing," so NSA requested DCI funds to produce videos to ensure all agencies provided Apex indoctrination briefings of the same quality (Harris, 1980, p. 2).[135]

In an internal memo, NSA leaders wrote that they wanted to "be a participant in successful resolutions to the many problems the community faces" but remained skeptical of Apex

[130] These accounts include interviews with people who had varying degrees of involvement in Apex and original source documentation from agency archives. We also included insights from oral history interviews conducted in 1993 by an agency's office of security.

[131] Information gleaned from interviews with two former security officers who had varying degrees of involvement with Apex.

[132] We were unable to find objective sources to definitively support or refute this belief.

[133] Need-to-know is a concept that requires people to share information only with those who need it to perform their jobs. Ever since the DCI issued DCID 8/1 on 4 June 2004, the applicability of need-to-know in interagency settings has been in question. Debate continues over the appropriate balance between need-to-know and the direction to provide all information IC customers need.

[134] Oral history interview conducted in 1993 by an agency's office of security.

[135] The standardization resulting from the indoctrination video would have benefited interagency work. However, consideration of the body of Apex information caused us to question the motive behind this funding request — was this agency encouraging consistency in the IC or resisting Apex implementation?

(Jenkins), 1979, p. 2). However, after the DCI informed NSA that the DCI would not provide funding for Apex, NSA leaders wrote to NSA's Apex Steering Group, "...it is in our interest to consider some alternative means of implementing Apex..." (Yeates, 1980, p. 1).

Industry representatives also opposed Apex.[136] Oral history interviews showed that industry representatives believed the cost of updating their software and administrative functions would be prohibitive.[137]

Industry representatives believed in the security control systems and the need-to-know concept. It is possible they were partially motivated by a desire to limit competition for future work in compartmented programs. In an era of extreme compartmentalization, few employees were cleared. Companies with employees cleared for a particular compartment had a business advantage over companies not cleared for it. Therefore, the industry representatives may have acted on a concern that Apex would take away their competitive advantage.

DCI Cancels Apex

DCI William Casey cancelled Apex on 5 March 1981 when he rescinded the portion of Presidential Directive/NSC-55 that established Apex (Leidenheimer, 1981, p. 1). Two interviewees believed that Apex died when Carter lost the Presidential election in November 1980. Even though the most senior ranks of the Carter administration supported Apex, there had been little commitment to it in the agencies.

Intelligence Community employees worked in a heavily compartmented, paper-laden environment in which the benefits of Apex were incomprehensible. They worked from hard-copy files, which were easily kept from view of employees not cleared to the specific program. An interviewee who worked on the Apex program shared this reflection:

> You could not get much information beyond what was physically in your office. There was no electronic search capability...The level of compartmentation made sense then. Just a few years later with electronic connections, Apex would have helped. We had blinders on. We had not experienced the future.[138]

Although the program was cancelled, the IC did benefit from Apex. Two security officers familiar with Apex reflected on the applicability of these lessons to current information sharing and security reform initiatives. They did not believe a single compartment was appropriate or tenable, but did identify some potentially useful changes. In 2007, the IC Chief Information Officer (CIO) launched an effort to formulate a master classification guide as part of its information sharing charter. One element under consideration was a matrix of thresholds for

---

[136] An agency's office of security conducted oral history interviews in 1993. Several government, military, and contractor employees shared their recollections of Apex, among other topics. These oral history interviews supplement the limited historical record for Apex. We point out that the agency conducted these interviews for a different purpose, and we did not ask the interviewees to validate their statements for accuracy or applicability to this study.

[137] Source: Oral history interviews conducted in 1993 by an agency's office of security.

[138] Interview with a security officer (2008) who worked on the Apex program.

various levels of sensitivity; threshold criteria were included in the compartmentation guidance for Apex.[139]

The IC Salvages Two Apex Projects

Apex was so complex that only two of its planned projects survived program cancellation. The Intelligence Community chose these projects to simplify disparate and labor-intensive visitor control processes.[140] The first project, the Community-wide, Computer-assisted, and Compartmented Control System (4C), was a government-wide database of clearances and accesses. The IC implemented 4C, but not to its full potential.

Security offices reportedly understood before 1974 that the IC adopted 4C as a Community goal (Eisenbeiss, 1981). The plan for 4C required agencies to store enough information to enable other security offices to verify that their employees had a current clearance.[141] In one respect, 4C was more complex than badge interoperability: sixteen agencies implemented 4C, but only five were involved in implementing badge interoperability (4C, 1980, p. 4).

The IC planned to begin deploying 4C in February 1982 and release the final version in September 1982. But concerns about compiling data in a single system and the accuracy of the data lingered. Agencies voluntarily updated their data by uploading their data or entering corrections manually. Because the data was not always current, security officers could not verify a visitor's clearance with much degree of certainty. Therefore, they likely used their best personal judgment to decide whether or not to let a person in.[142] Agencies fell behind in their data updates and system use dropped over time.[143]

The IC also salvaged the common badge for IC government employees from Apex to reduce their security costs and complexity. It took several more years for agencies to reach the next step in the 1990s — badge reciprocity. The IC will realize the full potential of the common badge once all agencies are fully interoperable. The interim success of completing Phase One of badge interoperability in April 2007 represented a significant interagency achievement (Director of National Intelligence (McConnell, 2007).

Badge Reciprocity: Adopting a Common Badge (1993)

Policymakers questioned the effectiveness of the IC and their adherence to law in the 1980s, a trend that had also occurred in the early 1970s. For example, the "Iran-Contra" scandal, which concluded in the late 1980s, added to the persistent belief that the Intelligence Community

---

[139] These recollections came from three e-mails written by long-time security officers with over twenty years of experience in the Intelligence Community (provided by a member of the IC Classification Marking Implementation Working Group).

[140] Interviews with two individuals with varying degrees of involvement with Apex and reciprocity.

[141] Including facility locations in the 4C database was controversial because of the classification of certain facilities.

[142] Source: Interview with a tiger team member.

[143] Source: Oral history interview conducted in 1993 by an agency's office of security.

lacked sufficient oversight.

Sources outside the Intelligence Community published details of so-called "intelligence failures." These publications contributed to perceptions that the IC was ineffective. According to one such source, the IC failed to anticipate the consequences of the Soviet Union's withdrawal from Afghanistan in February 1989 (Weiner, 2007, pp. 421-422). However, unclassified sources from authors inside the IC suggest that intelligence experts not only predicted the Soviet withdrawal and consequences but that these experts struggled to gain support from policymakers in Washington, D.C. (Schroen, 2005, pp. 55-56). Despite the existence of early intelligence information regarding Afghanistan, the perception of "intelligence failures" persists.[144]

The end of the Cold War altered the fundamental purpose and mission of the IC. Instead of the clearly defined target (i.e., the Soviet Union), the intelligence agencies warned senior policymakers about numerous decentralized threats, such as the emergence of Islamic terrorism. Views about the IC's response to this changing geopolitical environment differ based on whether an author worked inside or outside the IC. In addition, the CIA struggled with President William Clinton's skepticism of its covert operations. In 1996, a "failed covert action program that targeted Saddam Hussein embarrassed and frustrated the White House" (Coll, 2004, p. 353).

Significant shifts in the previously small IC workforce were also taking shape. Studies conducted during the Clinton administration concluded that outsourcing was cheaper than hiring government employees. Therefore, agencies across the government began downsizing and using contractors to supplement their workforce. Because the number of contractors had been small, some government staff did not fully trust contractors. The post-9/11 hiring surge of both government and contractor staff further increased the workforce and strained existing work patterns and policies, especially those involving security clearances and badges.[145]

IC Establishes the "One" Courier Badge (1991)

In 1991, the IC was significantly more insular than it is today — even couriers had trouble moving between agencies' compounds. A CIA security officer sorted out the courier issue and created the "One" Courier Badge for use at all IC agencies. Although this badge today seems like an obvious solution, at the time many organizations would have been leery of the badge if they suspected another agency controlled the process.

To deflect attention from the sample badge being printed on CIA stock and lighten the mood of some IC security managers, the CIA security officers "developed a sample orange

[144] During the period after a widely publicized "intelligence failure," public perceptions of ineffectiveness may harden. Simply releasing documents or information may not be enough to counter these perceptions.

[145] Source: interview with a long-serving IC employee who was affected by, but did not have direct involvement with, badge reciprocity.

badge with a picture of cartoon character Bart Simpson."[146] The security managers obtained approval from other agencies and issued the first IC-wide badges–the orange "IC Courier Badge." The courier badge was mostly a success, although certain facilities, such as the Pentagon, still required that couriers obtain one of their badges.[147]

Interest in a Common IC Badge Grows (1993)

After the Soviet Union collapsed and the Cold War ended in 1991–1992, many government leaders questioned the relevance of the IC. They demanded cuts to the IC's budget and staffing. The IC initiated badge reciprocity soon after these events began, but exact dates are not known.

The formal record for badge reciprocity begins in 1993, when the NSA and CIA formed the Community Access Control Working Group (later simplified to the Access Control Working Group, or ACWG). According to an internal memorandum for the record, representatives of the intelligence agency badge offices self-formed the ACWG to collectively respond to the DCI-sponsored Security Forum and Security Commission's concerns about access control practices. The ACWG's purpose was based on two assumptions:

1. Community senior management will not tolerate traditional access control methods, and
2. Community organizations should act collectively, cooperatively, and uniformly treating Community members as employees and not visitors.
   (MS&O, 1993, p. 2)

The ACWG has made a lasting contribution to security in the IC. In 2008, 15 years after the badge office representatives voluntarily banded together, the ACWG remains an active group that helps shape security policy and practices. The ACWG pattern of regular meetings, open discussion, and group problem-solving created a pattern of success that sustained badge interoperability during difficult circumstances.

Agencies Sign First Reciprocity Agreements (Early 1990s)

Interviewees attributed badge reciprocity to an informal arrangement between three agencies (DIA, NPIC, and CIA) to facilitate employee visits between their facilities. Until technology would support automated badge validation, the agencies decided to visually recognize each others' existing badges for government employees.[148] The agencies signed a memorandum of

---

[146] Source: E-mail written in September 2008 by a security officer with over 25 years of experience in the IC. We included the information he provided on the "One" Courier Badge, even though it was not part of the direct progression of the interoperable badge, to illustrate the IC's pre-9/11 evolving interest in integration and sharing.

[147] Source: E-mail written in September 2008 by a security officer with over 25 years of experience in the IC.

[148] Interviewees said badge interoperability was impossible in 1993 due to technical limitations. It turns out that interoperability was possible. CIA and NSA established interoperability in 1994, although their systems limited it to 3,000 participants (CIA, 17 May 1994).

agreement, briefed their security directors, and launched limited badge reciprocity.

Badge reciprocity was established to facilitate interagency visits for IC government civilians and assigned military personnel. Participating agencies accepted the other agencies' badges as proof of a badge holder's identity and clearance. Agencies recognized the common badge as validation of the badge holder's identity, citizenship, and access to TS//SCI material. The local security office issued the employee a Visit/No Escort badge, which enabled him or her to enter common areas of the facility.

From the beginning of reciprocity, the agencies planned to modify their existing automated access control systems to support a Community-wide badge system. Their purpose was to support "controlled but unencumbered access to sensitive (SCI) Community facilities by authorized Community personnel" and "eliminate the visit certification process for authorized Community employees" (National Reconnaissance Office (NRO), Management Services and Operations (MS&O), 1993, p. 2). In addition to simpler procedures, reciprocity ushered in a deeper change: belief that another agency's employees might be trustworthy.

Pressure to Simplify Security Intensifies (1994)

Director of Central Intelligence R. James Woolsey and Secretary of Defense William J. Perry chartered The Joint Security Commission (JSC) in June 1993 to examine security policies, practices, and procedures to make them simpler, more standard, and more cost effective. The report, published in February 1994, outlined the mismatch between security practices of the Cold War era and the rapid growth of technology and projected shifts in threat. The JSC assessment stated that agencies had "too many layers of physical security and they cost too much money" (Joint Security Commission, 1994, p. 18).

According to the Facilities Access Working Group, the JSC believed that the processes for passing clearances and registering and validating them were cumbersome (Facilities Access Work Group, Facilities Protection Committee of the Security Policy Board, 1998, p. 2). The number of employees impacted by the administrative process was small and decreasing because of downsizing in the 1990s. In addition, few missions required employees, especially contractors, to attend meetings at other agencies. However, the JSC still set the goal of implementing a standard IC badge.[149]

An NSA employee proposed a standard badge design that would simplify visual recognition for the security guards.[150] The proposed format provided a blue background indicating government employee and the employee's picture, name, and agency seal (Facilities Access Work Group, 1998, Annex 5). When the employee presented an approved badge, the agencies issued a local Visitor/No Escort badge to the visiting employee, and allowed him or her to enter

[149] The Commission did not reference the common badge initiative from Project Apex in the late 1970s.

[150] Interviewees said that the security guards would have to visually recognize multiple badge formats from these other agencies. Security officers were concerned about relying on humans to remember which agencies were participating. They agreed to a standard badge format and posting eligible badges at guard posts, which gave the guards a visual aid for comparison.

the facility without a prior visit request.[151]

The next stage of badge reciprocity agreements implemented the standard badge. The NSA, CIA, and DIA signed a memorandum of agreement in December 1995 to implement the Uniform Intelligence Community Badge, and other agencies gradually joined the program (NSA, 2003). Badge reciprocity functioned into the late 1990s. Agencies such as the NRO, CIA, and DIA declined to extend reciprocity to contractors. Their senior leaders reportedly were unsure that contractors would use their badges for official work purposes only, and not to use them to market their services directly to managers.

In a 2005 history developed for the Center for the Study of Intelligence, former CIA Historian Michael Warner attributed calls for greater efficiency to the IC budget and staffing cuts that occurred during the 1990s. The Aspin-Brown Commission reported that personnel costs grew to where they "crowded out investments in new technologies and limited operational flexibility" (Warner, 2005, p. 34). Security offices documented that "the Community resource climate to date" was unsupportive of investing in the Community badge, despite the outside forces advocating efficiency (NSA, 1995, p. 9).

One interviewee said that late 1990s studies into outsourcing government concluded that outsourcing was cheaper than hiring government employees. The CIA began significantly increasing its contractor ranks during the late 1990s. The Community continued its expansion after 9/11 with a hiring surge and increasing its use of contractors.

Funding Reciprocity

Agencies anticipated "...a direct relationship between ease of access and the basic costs (customer time) associated with the access control process" (National Security Agency, 1995, p. 7). They identified three factors that contributed to access control costs: visitor wait time, staff for the badge office, and staff for verifying clearances. The agencies believed that expanding participation to the whole Community would confuse the security guards, who performed visual badge inspections and would be unable to recognize numerous badges.

One senior security leader called badge reciprocity a "low or no-cost solution." Agencies expected the move to an interoperable badge would require substantial investment. In contrast to early stages of badge interoperability (2003-2004), agencies expected during badge reciprocity (early 1990s) that funding for the Community badge would come from their own budgets. "Funding for the initial study and technical evaluation...will be requested from the Security Forum; however, each organization will be required to independently fund specific changes and implementation methods..." (National Reconnaissance Office, Management Services and Operations (MS&O), 1993, p. 2).

The IC anticipated the danger of locking into outdated technology. The Uniform Intelligence Community Identification Badge Manual specified that "advanced technology solutions requiring substantial investment will be evaluated on their merits as they become

[151] A "Visitor/No Escort" badge allows a person to walk inside the local facility without having an escort. Some agencies kept a log of the "Visitor/No Escort" badge to provide limited audit capability.

available" (National Security Agency, 1995, p. 9).

They executed a low or no-cost solution. Badge offices printed posters with all eligible badges and posted them by the turnstiles at participating agencies. Security officers would match the presented badge to the poster. They would issue the visitor a "No Escort" badge, which enabled the other agency employee to walk into their facility without assistance.

Benefits of Reciprocity

Before badge reciprocity, agencies issued their own badges in isolation, and employees were subject to time-consuming administrative processes. Badge reciprocity freed intelligence officers from some administrative security processing and enabled them to devote more time to achieving the mission. Interviewees described instances when they had to pass clearances after reciprocity, causing them to question the effectiveness of badge reciprocity.[152] Badge reciprocity introduced gradual change to standard business processes, establishing a pattern that enabled later acceptance of badge interoperability.

An understated success of badge reciprocity was the 1993 founding of the ACWG. Fifteen years after the security badge offices self-started this body, members function as a single group to contribute to security policy and procedures. The ACWG pattern of meeting regularly for open discussion and group problem-solving created a pattern of success that sustained momentum for badge interoperability during difficult circumstances.

[152] Many of these instances were misunderstandings — the intelligence officers were attending meetings that required access to special compartments not included in badge reciprocity.

Retrospect and Outlook: Applicability of the Five Lessons

The unsuccessful attempts to develop interoperability in the 1970s and 1990s underscore the significance of successful completion of Phase One in 2007. Previous recommendations to reform the IC and attempts to implement a common IC badge call attention to the importance of badge interoperability. The five lessons of badge interoperability — commitment, complexity, diversity, staffing and additional duties, and adaptability — provide universal insights to organizational culture and human behavior.

These universal lessons anticipate the challenges likely when the IC brings the remaining 11 agencies into the program as planned in Phase Two of badge interoperability and beyond. We believe these lessons also pertain to interagency programs sponsored outside of security, such as building an integrated Intelligence Community architecture.

The lessons of badge interoperability echo the 1997 writings of the National Defense Panel:

> Transformation will take dedication and commitment — and a willingness to put money, resources, and structure behind a process structured to foster change. Most of all, it will take wisdom to walk the delicate line between avoiding premature decisions and unintended "lock-in" with equipment purchases, operational concepts, and related systems whose effectiveness may erode precipitously in a rapidly changing conflict environment. (National Defense Panel, 1997, pp. 57-58)

With an eye toward extending badge interoperability to additional IC agencies in future phases of badge interoperability, the security directors have several paths from which to choose, each with unique benefits and limitations. The security directors stated their desire to follow a path that meets the full requirements of the IC. The lessons of this study suggest that these requirements extend well beyond data fields and badge technology.

Numerous complexities make it debatable whether all intelligence agencies could share data from their current systems — adding data from additional disparate systems could yield still more variables that could break a fragile system. Unanticipated, non-technical complexities, such as agencies' concerns about committing the entire IC to a specific system or badge technology that will become outdated, require new approaches.

Future phases of badge interoperability are intricately related to development of a Community classification guide or reforming security clearance policies and processes. All five agencies agreed from the beginning about the benefit of badge interoperability. The execution challenges identified in Phase One illustrate the difficulty of identifying common standards, reaching compromises, and changing individual agency policies and practices.

Technical challenges will arise in just about any interagency venture and can be overcome with time. However, in Phase One of badge interoperability, we found that organizational culture and human behavior caused far greater challenges to the program. These universal

integration challenges will test other ODNI-sponsored initiatives, such as facilitating information sharing in the IC and training multidisciplinary teams of analysts to respond quickly to mission needs.

Appendix A. Methodology

This exploratory study examined Phase One of the Intelligence Community badge interoperability program, which lasted from October 2003 to April 2007. We designed this study to build a balanced, multidisciplinary picture of the program, from which lessons for the broader community could be derived.

Planning/Research

Our team of three researchers planned a research approach that would allow adequate time to explore challenging aspects of this interagency program.[153] We set the scope of research to a limited number of hypotheses, which would be revised during the study, as the data supported. We met informally with program leaders and reviewed extant data sources to learn program basics and clarify our preconceived topics of interest. The topics of interest were refined into research hypotheses, which shaped the data collection strategy.

To identify the events of badge interoperability, we interviewed government and contractor personnel who had expertise in different disciplines and who represented different levels of the agencies. Original source documentation, such as concept documents, memoranda, and e-mails, were to be used to clarify events and corroborate interview data.

We added research into past security-related interagency programs to our study as a means to look for patterns of organizational behavior. We compared a wide-reaching security program to smaller efforts targeted toward specific security objectives. To supplement interviews, we researched agency archives to find original source documents from these programs. We used academic journals to provide additional support for study findings.

Data Collection

The primary form of data collection was structured in-person interviews. We conducted a total of 30 interviews with government and contractor employees and used structured questionnaires tailored to four groups with distinct subject matter expertise and degrees of program involvement: tiger team, technical experts, budget/finance officers, and senior leaders.[154] We asked parallel questions of each group.

Two types of questions gathered different types of information. We used closed-ended questions to gather events, dates, and actions; open-ended questions drew out explanations and the interviewees' personal viewpoints.

[153] Three researchers were assigned to the study at the beginning. One researcher left the project after conducting a few interviews. Because other researchers with appropriate qualifications were not available, this person was not replaced. Instead, the other two researchers increased their level of support so they could complete the data collection, analysis, and writing.

[154] "Technical expert" refers to an individual who provided support to the databases, hardware, software, and communications, among other information technology components of the badge. "Senior leader" refers to an individual who held a position ranking above the tiger team. Examples include the security directors, agency-level directors, and directors from Community-wide programs and offices.

When requesting interviews, we provided topics that would be covered and asked the tiger team to identify attendees that had the right expertise. They typically selected interviewees based on their current or former positions. Some agencies opted to have small group interviews instead of individual interviews. The same questionnaires were used for both group and individual interviews. During group interviews, attendees clarified each other's responses and offered additional insights, but we did not ask each person individually to respond to every question.

Some agencies included both technical experts and tiger team members in their interviews. When attendees had mixed expertise, we referred to both questionnaires and verified that all questions relevant to their expertise were covered.

The initial interview yielded adequate detail from senior leaders and budget officers. However, we needed more details from the tiger team and technical experts. We developed new structured questionnaires to ensure parallel data collection on issues and discrepancies that arose during the initial interview. After the second parallel interviews were completed, we clarified specific details on an ad hoc basis.

Interview Procedures

We conducted all interviews in person, scheduling one and one-half hours to allow ample time for discussion. The duration of the interview was dependent on the interviewee's personality and the personal involvement with the program. Given the relatively small number of tiger team members and technical experts, complete confidentiality could not be assured. We informed all participants that their responses would be aggregated and any individual comments would be attributed to an agency, not to a person.

Most interviews were conducted by a pair of researchers. To prepare for the interviews, we reviewed the questions and verified together that we had the same understanding about their meaning. We took turns asking questions, and made contemporaneous notes throughout the interview. These notes were typed into a shared file as soon as possible after the interview to document the conversation.

Analytical Approach

We used interviews as the main source of data for this study, but ensuring reliability and objectivity presented us with some challenges. Interviewees' recollection of event details can fade, and personal perspectives change over time. During our research we identified conflicting accounts of some IC badge interoperability program events, which illustrated this challenge. In other cases we had concern that bias could become an issue with some interviews.

To deal with these research issues, we used more than one data source to corroborate interview data. We noted where more than one interviewee made the same point. In addition, we used data points from formal documentation (signed agreements and memoranda) and informal documentation (e-mails and handwritten notes) to support interview points.

We also assessed the data in terms of the interviewee's reliability. We determined whether the interviewee had first-hand knowledge (i.e., had personal knowledge of an event), or had second-hand knowledge (e.g., was told that an event happened, or read a memorandum).

Triangulation across diverse groups helped remove bias from the data. Using points made by more than one agency accounted for a single-agency perspective. Insights shared by groups having differing expertise (e.g., budget/finance as opposed to technology) were weighed more heavily than those made within a single expert group.

We supported data patterns and observations with findings of peer-reviewed literature from the business and management field. Using these expert sources, we revised our hypotheses and tested them against the data we uncovered. We also relied on themes from historical examples of security integration and collaboration to place all of the research themes in context.

From the themes, we developed preliminary lessons. We validated these lessons, as well as program milestones and timelines with a group of interviewees representing all participating agencies. Their feedback shaped later versions of the study lessons.

We presented the research themes and supporting data to a panel of interviewees on two occasions. We revised the themes and corrected data as appropriate.

Structuring the Lessons Learned Study

> "Lessons Learned" is the concept whereby an institution applies insights gained from its own or others' historical experiences in order to improve the conduct of its current and future activities. It has also been termed "experience-based insight." — *IC Lessons Learned Center website*

According to the above definition, the IC Lessons Learned Center views lessons learned as a continuous learning activity. Studies written from this perspective invite the reader to draw his or her own conclusions and determine how to conduct activities in the future. The developmental approach encourages agencies to learn from their successes and their mistakes, a key element of the National Intelligence Strategy, Enterprise Objective 9.[155]

For this study, the lessons, or findings, were structured in two parts. The first describes the conditions of the work activity, which might include observed events, behaviors, or factors. The second half of the study explains the effects the identified conditions had on the program.

To be presented as a lesson, both the condition and the effect had to be present. Some conditions indicated warning signs, but, because there was no observed effect on the program being studied, they were not presented as lessons. Even in situations for which the consequences were extreme, there was no lesson to be learned without an observed effect. In those cases, there was simply belief that the worst could happen, which does not provide a solid basis for change.

[155] *The National Intelligence Strategy*. Published by the Office of the Director of National Intelligence, October 2005.

The two halves of each lesson promote self-reflection, from which agencies decide how to proceed. The process of making conscious decisions to repeat certain activities and to make certain course corrections provides the learning called for in Enterprise Objective 9.

The finished study presented the lessons and explained their importance. Later sections provided supporting data from interviews and program documentation, support from peer-reviewed literature, and validation with historical insights. Footnotes were used throughout the document to cite sources, note discrepancies, and explain context where needed.

We sent the completed draft to CSNR and the ACWG for review and comment, incorporated revisions, and submitted a final draft to CSNR for acceptance. We delivered the final report to the DNI Lessons Learned Center. The Lessons Learned Center transferred the final report and all formal, original source program documentation to CSNR for archival processes.

Appendix B. Chronology of Phase One of Badge Interoperability

This table summarizes key events in the history of badge reciprocity and badge interoperability in the Intelligence Community. We derived these dates from hard copy and electronic source documents and interviews with personnel having first-hand knowledge of events.

Date	Event
8/1993	Representatives from badge offices across the IC form the Access Control Working Group (ACWG) to work on issues of common interest.
2/1994	Joint Security Commission recommends the IC develop a uniform badge system for the government's cleared community.
12/1995	Limited number of IC agencies sign a memorandum of agreement that establishes badge reciprocity between their headquarters facilities.
9/11/2001	Terrorists crash planes into the World Trade Center and the Pentagon.
10/31/2003	Director of Central Intelligence (DCI) George Tenet tasks the "Big Five" agencies with implementing badge interoperability within six months.
12/1/2003	Access Control Working Group (ACWG) representatives from applicable agencies have first meeting of the ICBIP sub-group.
1/21/2004	ICBIP sub-group members submit their initial cost estimates, which were based on a concept of translating data and sending it to the agencies.
3/11/2004	Counterintelligence experts assess badge interoperability and determine that the IC would benefit from the audit and tracking capability.
7/20/2004	ICBIP sub-group publishes the ICBIP schedule, which set a deadline of 12/31/2005.
7/22/2004	The 9/11 Commission releases its report on the Terrorist Attacks on the World Trade Center and the Pentagon; recommends improvements such as creation of a new Director of National Intelligence.
9/9/2004	EXDIR/ICA memo directs participating agencies to transfer funding to the technical lead agency to cover ICBIP startup costs.
9/24/2004	Porter Goss becomes the next DCI.
10/6/2004	ICBIP sub-group agrees to a standard for the personal identification number (PIN).

10/20/2004	Technical lead agency presents first briefing on the ICBIP concept to the Defense and Intelligence Community Accreditation Support Team (DICAST).
12/28/2004	EXDIR/ICA memo instructs agencies to reallocate resources to implement ICBIP before 12/31/2005.
1/12/2005	One agency achieves Approval to Operate (ATO) for its badge system, an important milestone for executing interoperability.
1/12/2005	One agency reports that its legacy badge system could not support other agency records because it was already at its design capacity.
2/16/2005	DNI Special Security Center asks agencies if they could meet the 12/31/2005 deadline; four of the five agencies said yes, but with caveats.
3/31/2005	The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (the "WMD Commission") reports its finding that pre-war judgments about Iraq's weapons of mass destruction were incorrect.
4/18/2005	Technical lead proposes an interim solution to enable one agency to participate despite issues with its legacy badge system.
4/19/2005	Security Directors from the participating agencies approve the final design for the interoperable badges.
4/21/2005	John Negroponte becomes the first Director of National Intelligence (DNI) and Porter Goss becomes Director, Central Intelligence Agency (D/CIA).
4/27/2005	Second agency achieves Interim Approval to Operate (IATO) milestone for its badge system, the minimum approval for executing interoperability.
5/18/2005	ICBIP sub-group agrees to begin visually accepting new badges in August 2005, as a temporary measure until they achieve interoperability.
12/15/2005	Technical lead makes a second briefing to the DICAST.
5/3/2006	DNI disbands the DICAST after the Intelligence Community (IC) Chief Information Officer (CIO) position and office are created.
5/12/2006	Third agency achieves the ATO milestone for its badge system.
5/26/2006	Porter Goss leaves the D/CIA position.
5/30/2006	Michael Hayden becomes the next D/CIA.
6/13/2006	A fourth agency achieves the IATO milestone for its badge system.

9/6/2006	Purple badge for members of Congressional staff approved; these badge holders can visit local facilities, subject to local entry procedures.
9/1/2006 - 10/31/2006	Participating agencies sign updated Interconnection Security Agreements with the technical lead.
10/16/2006	Intelligence Community Technology Governance Board (ITGB) requests documentation from each agency before approving ICBIP.
11/30/2006	Fifth agency achieves IATO for its badge system.
12/19/2006	ITGB issues IATO for four agencies.
1/17/2007	ITGB issues IATO for the fifth agency.
1/1/2007	ICBIP sub-group tests badges at all participating facilities during the first of two "Roadshows."
2/1/2007	ICBIP sub-group conducts the second of two "Roadshows" to test badges.
2/12/2007	John Negroponte becomes the Deputy Secretary of State.
2/13/2007	Michael McConnell becomes the new DNI.
3/1/2007	Director, DSSC makes final determination that ICBIP will include contractors.
4/18/2007	One of the agencies has not released its contractor records to the other agencies, despite D/DSSC's March decision.
4/23/2007	DNI announces successful completion of Phase I of the ICBIP.

Appendix C. The Intended Schedule for ICBIP: "Initial Program Timeline"

Phase 1 July – Sept 04 (4th Quarter - FY04)	Phase 2 Oct – Dec 04 (1st Quarter - FY05)	Phase 3 Jan – Sept 05 (2nd – 4th Quarters)	Phase 4 Oct – Dec 05 (1st Quarter - FY06)	Phase 5 Jan 06 –
Develop CONOP TL Brief DICAST (Begin Accreditation Process) Develop Badge Design Identify Hardware (Compatible Readers) Each Agency coordinate with TL to establish date conversion protocols	Each Agency Purchase Hardware TL Purchase IS Servers Establish Date Conversion Software Scripts	Begin Rebadging Installation of all hardware and software	Implement Badge Data Sharing	Incorporate Other IC Agencies
			Legend: IS = interoperability server TL = technical lead	

Note: The timeline is completely dependent on the timeliness of funding and each Agency's internal certification and accreditation process approvals.

References

4C Briefing to Apex Steering Group. (1980, 12 August). NSA Archives.

Access Control Working Group (ACWG). (2005, 12 January). ACWG Meeting Minutes. ACWG files.

Access Control Working Group (ACWG). (2006a, 22 June). ACWG Meeting Minutes. ACWG files.

Access Control Working Group (ACWG). (2006b, 21 August). ACWG Meeting Minutes. ACWG files.

Bardach, E. (2005). How Do They Stack Up? The 9/11 Commission Report and the Management Literature. *International Public Management Journal*, 8(3), 351-364.

Central Intelligence Agency (CIA). (1994, 17 May). *Employee Bulletin.*

Central Intelligence Agency (CIA). (1999, November). *At Cold War's End: U.S. Intelligence on the Soviet Union and Eastern Europe, 1989-1991.* Center for the Study of Intelligence.

Central Intelligence Agency (CIA). (2007, October). *Lessons Learned: Interagency Collaboration in Support of Operation Northern Exposure.* Center for the Study of Intelligence and the National Counterterrorism Center.

Coll, S. (2004). *Ghost Wars: The Secret History of the CIA, Afghanistan, and bin Laden, from the Soviet Invasion to September 10, 2001.* New York, NY: Penguin Press.

Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD Commission). (2005, 31 March). *Report to the President of the United States.* Washington, D.C.: Government Printing Office.

Community Interoperability and Information Sharing Office (CIISO). (2005, 20 October). *FY 2007-2011 National Intelligence Program (NIP) Assessment: Information Sharing Training.* CSNR Reference Collection.

Director of Central Intelligence Directive (DCID) 6/3. (2008, 15 September Replaced by ICD 503). *Policy, Protecting Sensitive Compartmented Information within Information Systems.* CSNR Reference Collection.

DCI Working Group on Compartmentation and Codewords. (1978, October). *Draft Report of the Working Group on Compartmentation and Codewords.* NSA Archives.

Eisenbeiss, Harry C. (1981, 11 February). Special Assistant to DCI for Compartmentation Memorandum for: Adm. Bobby R. Inman, D/NSA. Subject: 4C. NSA Archives.

Facilities Access Work Group, Facilities Protection Committee of the Security Policy Board. (1998, February). *Standard Badge for Government: White Paper with Memorandum of Agreement.* NSA Office of Security.

Fischer, Bill and Boynton, Andy. (2005, July). Virtuoso Teams. *Harvard Business Review.* Cambridge, MA: Harvard Business School Publications.

Gratton, Lynda and Erickson, Tamara. (2007, November). Eight Ways to Build Collaborative Teams. *Harvard Business Review.* Cambridge, MA: Harvard Business School Publications.

Haines, G. (1999, Winter) Looking for a Rogue Elephant: The Pike Committee Investigations and the CIA. *Studies in Intelligence*, Winter 1998-1999. Langley, VA: Central Intelligence Agency.

Harris, A. K. (1980, 9 June). Chief, M56 Memorandum for: Chief, VI. Subject: Request for Excess 4C Funds. NSA Archives.

Heifetz, Ronald and Laurie, Donald. (2001, December). The Work of Leadership. *Harvard Business Review.* Cambridge, MA: Harvard Business School Publications.

Inman, Adm. Bobby R. (1980, 17 October). D/NSA Memorandum for: the DCI for Resource Management. Subject: Resource Request for Apex Implementation. NSA Archives.

Jenkins, William H. (1979, August). DDO (NSA) Memorandum for: D/NSA, Admiral Bobby R. Inman. Subject: NSA Alternative — Presentation to Walsh Committee. NSA Archives.

Joint Security Commission. (1994, February). *Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence.* Washington, D.C.: Joint Security Commission.

Katzenbach, Jon and Smith, Douglas. (2005, July). The Discipline of Teams. *Harvard Business Review.* Cambridge, MA: Harvard Business School Publications.

Kotter, J. (2007, January). Leading Change: Why Transformation Efforts Fail. *Harvard Business Review.* Cambridge, MA: Harvard Business School Publications.

Leidenheimer, Robert E. (1981, 9 July). Special Assistant to DCI for Compartmentation Memorandum for: Members of DCI Committee on Compartmentation. Subject: Disposition of APEX Training/Administrative Materials. NSA Archives.

Management Services and Operations (MS&O), National Reconnaissance Office. (1993, 26 August). Memorandum for the Record. Subject: Participation on the Community Access Control Working Group. ACWG files.

Management Services & Operations (MS&O), National Reconnaissance Office. (2003, August). Memorandum for the Record. Subject: Participation on the Community Access Control Working Group. MS&O files.

McConnell, Mike. (2007, 20 April). DNI Letter to: Intelligence Community Colleagues. Subject: Intelligence Community Badge Interoperability Program. ACWG files.

Mintzberg, Henry. (1994, January). The Fall and Rise of Strategic Planning. *Harvard Business Review.* Cambridge, MA: Harvard Business School Publications.

Nagy, D. (2000). A Military Intelligence Knowledge Base and Knowledge Management: Cultural Factors. *Defense Intelligence Journal,* 9(1), 39-56.

National Defense Panel. (1997, December). *Transforming Defense: National Security in the 21st Century.* CSNR Reference Collection.

National Foreign Intelligence Board (NFIB). (1978, 27 October). Memorandum for: National Foreign Intelligence Community. Subject: Compartmentation and Security. NRO Archives.

National Foreign Intelligence Program (NFIP) Working Group on Compartmentation. (1979, May). *The APEX Special Access Control System.* NRO Archives.

National Reconnaissance Office (NRO). (1993, November). *The BYEMAN Security System – A Historical Perspective, Volume II.* (**Note: these oral history interviews were conducted for other purposes.) NRO Office of Security and Counterintelligence.

National Security Agency (NSA). (1995, 30 January). *Uniform Intelligence Community Identification Badge Manual.* NSA Office of Security.

National Security Agency (NSA). (2003, 15 January). *Interfacing with the Intelligence Community Badge System (ICBS).* NSA Office of Security.

O'Neill, Alan and Jabri, Muayyad. (2007). Legitimation and Group Conversational Practices: Implications for Managing Change. *Leadership and Organization Development Journal,* 28(6), 571-588. Emerald Group Publishing, Ltd.

Office of the Director of National Intelligence (ODNI). (2005). *National Intelligence Strategy.* CSNR Reference Collection.

Office of the Director of National Intelligence (ODNI). (2008a, August). *Intelligence Community Policy Guidance (ICPG) 105.3: Acquisition Workforce Policy.* Draft document (Assistant Deputy Director of National Intelligence and Senior Acquisition Executive). CSNR Reference Collection.

Office of the Director of National Intelligence (ODNI). (2008b, 15 September). *Intelligence Community Technology Systems Security Risk Management, Certification and Accreditation (ICD 503).* CSNR Reference Collection.

Ostroff, F. (2006, May). Change Management in Government. *Harvard Business Review.* Cambridge, MA: Harvard Business School Publications.

Presidential Directive/NSC-55. (1980, 8 January). Subject: Intelligence Special Access Programs: Establishment of the Apex Program. *National Archives Online.*

Public Key Cryptography. *Intellipedia,* (2008, August). Retrieved 7 August 2008.

Schroen, G. (2005). *First In: An Insider's Account of How the CIA Spearheaded the War on Terror in Afghanistan.* New York, NY: Ballantine Books.

Sirkin, Harold; Keenan, Perry; and Jackson, Alan. (2005, October). The Hard Side of Change Management. *Harvard Business Review.* Cambridge, MA: Harvard Business School Publications.

Tiger Team Meeting Minutes, 22 June 2006. ACWG files.

Turner, M. (2005). *Why Secret Intelligence Fails.* Dulles, VA: Potomac Books, Inc.

United States Intelligence Board (USIB). (1975, 22 December). *Security Committee Task Force Report on Compartmentation.* NSA Archives.

United States National Commission on Terrorist Attacks Upon the United States (9/11 Commission). (2004, July). *The 9/11 Commission Report.* Washington, D.C.: Government Printing Office.

Vlaar, Paul; Van den Bosch, Frans; and Volberda, Henk. (2007, August). On the Evolution of Trust, Distrust, and Formal Coordination and Control in Interorganizational Relationships: Toward an Integrative Framework. *Group and Organization Management,* 32(4). Sage Publications.

Warner, M. and McDonald, J. K. (2005, April). *U.S. Intelligence Community Reform Studies since 1947.* Center for the Study of Intelligence.

Washington Roundup: Intelligence Shifts. *Aviation Week and Space Technology.* (1980, 24 November).

Weiner, T. (2007). *Legacy of Ashes: The History of the CIA.* New York, NY: Doubleday.

Yeates, Eugene F. (1980, 7 November). NSA, Chief, Office of Policy Memorandum for: Chairman & Member NSA Apex Steering Group. Subject: APEX — Our Implementation Alternative. NSA Archives.