(b)(7)(E)

Banner redactions pursuant to (b)(7)(E)
FBI

15 April 2010

Report to the Director of National Intelligence on the Fort Hood and Northwest Flight 253 Incidents (U)

Intelligence Community Review Panel

(b)(3)

CL BY: [redacted]
CL REASON: 1.4 (b), (c), (d)
DECL ON: 25X1-human
DRV FROM: Multiple Sources

(b)(7)(E)

Report to the Director of National Intelligence on the Fort Hood and Northwest Flight 253 Incidents (U)

Executive Summary (U)

(b)(1)
(b)(3)
(b)(7)(E)
FBI

[redacted] ~~(S)~~

"In a way, I think this Christmas Day bomber did us a favor."

—Gov. Thomas H. Kean, 25 January 2010.[1]

The Director of National Intelligence (DNI) asked a panel of four senior current and former national security officials in January to examine the intelligence aspects of two recent events: the shooting attack on personnel at Fort Hood by Army Major Nidal Hasan on 5 November and the attempted bombing of Northwest Airlines Flight 253 on Christmas day by a Nigerian citizen, Umar Farouk Abdulmutallab.[a] (U)

The panel's mandate was three-fold: To document the facts of these two events, to add recommendations to what the Intelligence Community is doing in response to them, and to add any further thoughts on what the Intelligence Community might do to deal with existing terrorist threats or what form new terrorist threats might take. (U)

To carry out this assignment, the panel read all of the relevant intelligence reporting and carried out roughly 70 interviews, meetings, and roundtable discussions with approximately 300 key decision makers, program managers, officers, and agents from components in the Office of the Director of National Intelligence (ODNI), the National Counterterrorism Center (NCTC), the Central Intelligence Agency (CIA), including its Counterterrorism Center (CTC), the Defense Intelligence Agency's (DIA)

[a] Panel members were the Honorable John McLaughlin, former Deputy Director of the Central Intelligence Agency; Mr. Dale Watson, former Executive Assistant Director for Counterterrorism and Counterintellligence at the FBI, and the first FBI deputy director at the CIA's Counterterrorism Center; Dr. Peter Weinberger, a senior scientist at Google and a member of NSA's external advisory board; and Mr. Alexander Joel, an attorney serving as Civil Liberties Protection Officer in the Office of the Director of National Intelligence. (U)

Joint Intelligence Task Force-Counterterrorism (JITF-CT), the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), the Department of Homeland Security (DHS), the Office of the Undersecretary of Defense for Intelligence, and the National Security Council. It also asked a panel of experts from outside the Intelligence Community to offer ideas on future threats and called on four external readers—a scholar, the head of a major research institution, and two former senior intelligence officials—to critique the study. (U)

Before summarizing the findings, some preliminary observations are in order regarding the context in which the panel encourages readers to evaluate its findings. (U)

First, the panel was struck by the enormous complexity of these issues and the challenges facing intelligence and law enforcement officers who must wrestle with them. The panel tried to evaluate these events dispassionately and clinically and, although it judges many actions critically, it is fully aware that whatever shortcomings it found are not typical of the Intelligence Community's overall performance on counterterrorism.

- We saw our work as roughly akin to an FAA assessment of an airline accident in which a single plane crash is seldom seen as emblematic of an industrywide problem—so it is with these events and the Intelligence Community.

- Our simple aim was to develop a clear-eyed view of how the Intelligence Community's counterterrorism performance can become even better and how the adversary's task can be made harder. (U)

Second, it is important to understand the context for the Intelligence Community at the time of these events. During our review, we were consistently impressed by the pace, scope, breadth, and depth of US counterterrorism efforts throughout 2009, many of which produced notable successes. Intelligence and law enforcement officers were tracking threats or supporting operations to counter them in Pakistan, within the United States, Southeast Asia, and the Persian Gulf. They were [redacted] fielding multiple requests for briefings; coordinating action with collectors, policymakers, and the law enforcement community; and providing analysis and support following the June shootings at a US military recruiting center in Little Rock, Arkansas. (b)(1) (b)(3)

(b)(1)
(b)(3)
NSA

- Analysts tracking Yemen estimated that they received approximately 500-700 pieces of relevant traffic daily; [redacted]

(b)(1)
(b)(3)
(b)(7)(E)
FBI

- [redacted] ~~(S//OC/NF/~~ [redacted]

(b)(1)
(b)(3)
NSA

Third, based partly on this surfeit of data, the panel concluded early on that it is too simple to call the challenge in these cases a "connect the dots" problem—a metaphor that strips away context and trivializes the challenge counterterrorism officers face in dealing with truly massive volumes of information. The 25 December case in particular is more akin to what scholar Roberta Wohlstetter in her classic study of Pearl Harbor called the "signals to noise" problem. In short, the fragmentary clues about Abdulmutallab—the "signals"—were deeply submerged in a vast pool of intelligence reporting—thousands of messages a day, the "noise."

- The task then, and the North Star guiding this panel's efforts, has been the question of how to raise such alarming "signals" from a body of noise that is growing rapidly as technology enables both the creation of more data and the Intelligence Community's ability to collect it. (U)

Fourth, while perfection should be the goal for counterterrorism, there is really no formula to achieve it. Terrorists are "learning" enemies; they go to school on every one of our successes, play by no rules, do not respond to traditional deterrence techniques, and are prepared to die to achieve their aims. So while the recommendations we offer and the steps the Community has already taken will reduce the odds of terrorist success, no one can guarantee that terrorists will not penetrate our defenses on some occasion. (U)

Finally, in considering any set of recommendations on counterterrorism, it is important to remain aware that major changes will require tradeoffs—fiscal, bureaucratic, and so on. For example, [redacted] Easing standards for placing suspicious people

(b)(1)
(b)(3)
NSA
CIA

on various airline watchlists will produce a surge of false positives; using partial names to increase the likelihood of detecting terrorist travel risks compromising sensitive collection programs by which the Community [redacted] ~~(S//NF)~~ (b)(1) (b)(3)

What Happened? (U)

The first task the DNI gave the panel was to determine the facts in these two cases. This is elaborately laid out in the first section of the report, in which we document chronologically what occurred, what advance intelligence reporting was available, and what intelligence and law enforcement officers did or did not do with it. There and throughout our report, we focus in more detail on the 25 December attempted bombing than on the Fort Hood shooting. Because ongoing legal proceedings limited our access to personnel and data associated with the Fort Hood case, we relied heavily on the joint preliminary review conducted by the Department of Defense (DoD), FBI, and ODNI, and a separate DoD inquiry. Moreover, as we undertook this assignment, another group led by former CIA and FBI Director William Webster began an in-depth study focused on FBI's role in the Fort Hood case. (U)

To summarize what we learned about the nature of the intelligence reporting:

- There were multiple reports leading up to the 25 December event, mostly [redacted] (b)(1) (b)(3) NSA
- [redacted] (b)(1) (b)(3) NSA (b)(1) (b)(3) (b)(7)(E) FBI
- [redacted] (b)(1) (b)(3) NSA

(b)(1) (b)(3) NSA

[redacted] ~~(TS//HCS/SI//NF)~~

Counterterrorism officers were up against some tough challenges in assessing the implications of this reporting. Regarding the 25 December event, the panel nonetheless believes that analysts and collectors could have pursued strategies that would have raised Abdulmutallab out of the "noise" or possibly even pointed to his target and timing. (U)

(b)(1) (b)(3) NSA CIA

Had certain messages been put together—[redacted] and [redacted] reporting the concerns of Abdulmutallab's father—officers would have assembled Abdulmutallab's full name, his biographic data, and his association with Aulaqi. This would have put him on officers' screens for more follow-up.

- However, [redacted] the CIA [redacted] unit most focused on the Abdulmutallab case—did not receive [redacted] message that linked him to Aulaqi. Meanwhile, name traces done in Washington searched databases that did not contain that [redacted] message. As a result, no one connected Abdulmutallab to Aulaqi and his hostile aims toward the US.

(b)(1) (b)(3) CIA

(b)(1) (b)(3) NSA

(b)(1) (b)(3) NSA

- [redacted] ~~(TS//HCS/SI//NF)~~

(b)(1) (b)(3) NSA CIA

[redacted]

(b)(1) (b)(3) NSA CIA

- [redacted] ~~(TS//SI//NF)~~

(b)(1)
(b)(3)
NSA

[redacted] ~~(S//NF)~~

(b)(1)
(b)(3)
FBI

(b)(1)
(b)(3)
NSA

(b)(1)
(b)(3)
FBI

(b)(1)
(b)(3)
NSA

[redacted] ~~(S//NF)~~

The panel recognizes that laying things out this way makes counterterrorism sound easier than it is in the real world of burgeoning volume, competing priorities, and the attendant increase in "noise." We would be irresponsible, though, to simply conclude that detection in this case was impossible, unlikely, or that these cases were below the threshold. Our key point is simply that it was possible to find the connections; the recommendations we summarize below and elaborate in the report are geared to increasing the odds of that happening in the future. (U)

(b)(1)
(b)(3)
(b)(7)(E)
FBI

[redacted] ~~S//OC/NF~~ [redacted]

(b)(1)
(b)(3)
NSA

(b)(1)
(b)(3)
(b)(7)(E)
FBI

[redacted]

(b)(1) (b)(3) (b)(7)(E) FBI

[redacted]

(b)(1) (b)(3) (b)(7)(E) FBI

- [redacted] (b)(1) (b)(3) NSA

(b)(1) (b)(3) (b)(7)(E) FBI

- [redacted] ~~(S//OC/NF~~ [redacted] (b)(1) (b)(3) (b)(7)(E) FBI

(b)(1) (b)(3) (b)(7)(E) FBI

[redacted] (b)(1) (b)(3) NSA

(b)(1) (b)(3) (b)(7)(E) FBI

- [redacted]

(b)(1) (b)(3) (b)(7)(E) FBI

- [redacted] ~~(S//OC/NF/~~[redacted]

What Needs to be Done? (U)

Anyone studying these two cases can be tempted to conclude that they resulted from simple procedural errors and that reoccurrences can be prevented with a few easy fixes. [redacted] In the case of the State Department, a single keystroke leaving out one letter of Abdulmutallab's name—in a computer program not then configured to compensate for error—masked his possession of a valid US visa. Knowing

(b)(1) (b)(3) NSA CIA

(b)(1)
(b)(3)
(b)(7)(E)
FBI

he had a visa would probably also have pulled him up out of the "noise." [redacted] ~~(S//HCS//OC/NF/~~[redacted]

Alluring as it is to think the problems can be solved with such mundane procedural steps, the panel concluded that reducing the chances of reoccurrences requires much more. The panel was heartened to discover that the Community has indeed "gone to school" on these two cases; we counted over a hundred separate proposals for improvements in various stages of study or implementation. (U)

So in formulating our recommendations, the panel is aware that we are dealing with a moving target. We are convinced, however, that in most areas our diagnosis of problems and our recommendations go beyond or build on what the Community is doing or planning. We believe these must be pursued with the urgency they would have if NW 253 had blown up in the sky above Detroit on Christmas. Nothing the US Government did prevented that from happening. (U)

A full list of our recommendations follows in Appendix A. Our recommendations fall into four broad categories. (U)

First, the Community needs more efficient internal processes for locating, retrieving, and disseminating terrorism-related intelligence that may be submerged in "noise"—and some new business practices for how the Community uses that intelligence once it has been identified. Agency heads have already embarked on much of this—directing, for example, changes that require more rapid sharing of reports, updating of dissemination lists, more rigorous visa checks, and all-source approaches to name tracing. (U)

A closely related part of this is the equally important issue of watchlisting—how analysts use and collate raw reporting to identify a potential terrorist and prevent him from entering the United States. Watchlisting has improved dramatically since 9/11, but the panel nonetheless believes there are still some important gaps to close. (U)

The essence of the problem is that the process is too segmented and that no single individual or entity has full end-to-end responsibility for a particular nomination. Everyone works very hard at it, but we found considerable confusion among the agencies about roles, responsibilities, and procedures. As a result, few participants have a fully informed substantive grasp from

start to finish. At each step of a multi-layered process, someone assumes that someone else took the hard substantive look or did the thorough digging that is required in watchlisting cases. (U)

We saw this glaringly in the Abdulmutallab case; it is only a matter of time before similar instances occur. (U)

Our report addresses in some detail the question of whether Abdulmutallab could have been kept off Flight 253 by designation for the "No Fly" list. We encountered strongly competing views on this, with data that can be marshaled on both sides. Our bottom line is that the intelligence was present to nominate him for the "No Fly" list; we are less certain that the nomination would have been approved, given differing interpretations of the criteria at the time. Our fuller view of this is described in the textbox on page 19. (U)

Related to all of this is what we found to be ambiguity surrounding the Terrorist Identities Datamart Environment (TIDE)—the database that is commonly thought to be the broadest repository for data on people of possible terrorist concern. The panel concluded, however, that in practice TIDE is really a compilation of individuals who have been considered for watchlisting; people who fall below that threshold but who nonetheless merit concern are not necessarily included. This limits TIDE's utility as a tool that analysts populate with fragmentary data to build, identify, and shape a dossier on a suspected terrorist. (U)

To summarize our recommendations in this area, the Community should:

- ***Clarify the criteria for watchlisting in a way that does not become excessively specific, onerous, and legalistic;***

- ***Establish a training program that will provide greater clarity on the roles and responsibilities of every agency in the watchlisting process;***

- ***Instruct analysts to populate TIDE with partial derogatory information—making TIDE "the place to build a dossier"—rather than treating it as a library of completed watchlist nominations. (U)***

The second major set of recommendations concerns the need for an information architecture that reduces the "signals to noise" ratio for analysts rather than magnifying it. This has been seen as a problem for years but the Community is still far away from uniform or broad

application of the search and correlation capabilities available in the private sector or in the average US home. (U)

Slow progress on this is always attributed to the tensions between the need to share information versus the need to protect it. Many of these problems are understandable, but if the Community does not push through these barriers it guarantees that we will have more surprises like Abdulmutallab's attempted attack. (U)

The absence of adequate information technology runs through both the Fort Hood and Flight 253 narratives, particularly the inability of information systems to help analysts locate relevant reporting in a sea of fragmentary data or to correct for seemingly minor human errors. This, despite the existence throughout the Community of several excellent systems run by specific agencies or focused on a specific problem—but either not broadly available or broadly applied. (U)

Our recommendations call for actions in the near term, the medium term, and the longer term—in an effort to put information technology objectives into a strategic context. (U)

In the near term, the priority should be on a problem we saw in both cases—that many officers do not know what data exist and how to access it or use it. Examples of things that could be done include: greatly increasing online documentation on what is available, how to get access, who has access, and tips from experienced users; embedding information specialists in fast-moving analytic or operational groups to handle support requests immediately; ensuring that all systems default to "fuzzy logic" to help correct for imprecision or errors in searches; implementing the DNI's decision to support near-term enhancements to a particularly sophisticated CIA analytic tool to enable National Counterterrorism Center (NCTC) and CIA officers to use its unique capabilities with limited technical assistance. (U)

In the medium term, but sooner rather than later, the Community must enable persistent search, attach analytic insights to data, and bridge the divides that separate datasets. For example, intelligence officers need user-controlled alerting services that can flag incoming traffic and correlate it with existing reporting—a capability that could have linked communications between Aulaqi and Hasan as they arrived. Officers need to be able to see who else has looked at a report, attach comments electronically, and see what others think—a capability that would have enabled broader discussion among analysts interested in an unnamed

Nigerian affiliated with Aulaqi. And it is critical to incorporate into all programs tools that enable officers to access multiple databases across multiple networks through a single software interface. (U)

Over the longer term, the Community needs to push completion of state-of-the-art search and correlation capabilities, including techniques that would provide a single point of entry to query databases for which officers have authorized access. We endorse the joint efforts of various agencies to build toward a common information infrastructure with common data services, such as those for collaboration, access, discovery, audit processing, and storage. (U)

A critical step would be to establish the virtual equivalent of the now-common Community badge—that is, a uniform way across the Community of identifying logged-in individuals and their access permissions, together with tagging of data to describe the rights needed to access it. This is probably the key step needed to break through the barriers to sharing that result from legitimate concerns for protection of sensitive data. (U)

Intelligence Community Directive 501, which codifies procedures for discovery and sharing of data, effectively lays the policy groundwork for implementing our recommendations on information technology. (U)

To summarize our recommendations in this area:

- ***In the near term, take steps to ensure that counterterrorism officers understand all of the data available to them and have the tools simply to access efficiently what already exists—when they need it and where they need it.***

- ***In the medium term, augment capabilities to get more out of information with tools that allow officers to learn more from the data than what it presents on the surface—who has seen it, what others think of it or have done with it, what related data are available, and how it relates to historical reporting.***

- ***In the longer term, move beyond an architecture that relies so heavily on human initiative to one in which "data can talk to data"—so that relationships embedded in complex datasets are brought to the surface in ways that move the analyst's starting point further down the field and closer to discovery of an adversary's plans and intentions.***

- ***Pursue these objectives on a "crash" basis. The panel is convinced that delay will assure that more Umar Farouks get through US defenses. (U)***

The panel's third set of concerns and recommendations has to do with closing or bridging the structural seams in the counterterrorism mission. The "seams" are visible in numerous ways—in the blurred distinctions between the NCTC and CIA missions, uncertainty about primary responsibility for homeland-related issues, and an underdeveloped appreciation for the benefits of "jointness" in some mission areas. (U)

We began this study thinking that the redundancies in the Community's counterterrorism efforts represent healthy competition and that "lanes-in-the-road" issues in no way directly contributed to the Fort Hood or 25 December incidents. Officers we interviewed consistently said that turf considerations and bureaucratic overlap did not play a direct role in either incident. (U)

There is no way for the panel to produce a definitive assessment on that point, but there are grounds for skepticism. Generally, the panel thought the competition for primacy on many issues between CIA's Counterterrorism Center (CTC) and NCTC, for example, needlessly diverts the creative energy and resources of both organizations. Both organizations are staffed by highly dedicated officers and both have enjoyed impressive successes. But the panel thinks this competitive climate contributes to the "signals to noise" problem—given that finding the "signals" is highly labor and detail intensive—and could hamper the Community's ability to detect and prevent the next Abdulmutallab-like attack. (U)

Managing this competition has been a perennial problem since the creation of NCTC in 2004 and flows from the overlap in the analytic responsibilities of the two organizations and their need to draw mainly on the same talent pool. The panel discussed the merits of merging the two organizations' analytic functions, but concluded that important distinctions in areas ranging from legal authorities to data access argue against that. (U)

NCTC's unique access to homeland data, its legislative authorities, and its relationship to the FBI make it the natural lead on all threats with potential to reach US soil. CIA/CTC on other hand is the natural lead on terrorist operations abroad, particularly involving support to operators and collectors. We cannot improve on a recent DNI directive that captures

these distinctions and embodies many of the views the panel has expressed in its meetings with NCTC, CTC, and the DNI (See Appendix D). (U)

There have been numerous such efforts to clarify the "lanes in the road" over the years, however, and in the end it will be a leadership and management responsibility to ensure that each organization plays to its comparative advantage. (U)

Related to that, the panel sees a need to dramatically increase the focus on threats to the homeland. We believe that the segmented nature of the counterterrorism community and the fragmentary quality of the data require a singular focus by some unit on unearthing such plots. In our view, this should be the primary mission of NCTC's new "pursuit" effort, which is focused on more fully developing fragmentary data that raise concerns about terrorism but lack specificity. We applaud this effort, which must avoid the temptation to put the bulk of its energy into the more familiar task of tracking threats overseas. (U)

To summarize our recommendations in this area:

- ***Organizational responsibilities should play to the clear strengths of each organization. NCTC's relationship with FBI, its legislative authorities, and its tie-in to the homeland make it the natural lead on all threats with the potential to reach US soil. CTC's natural strength is in focusing on terrorist operations abroad, particularly involving support to operators and collectors.***

- ***Counterterrorism organizations must each maintain both a tactical and strategic focus. They are mutually reinforcing emphases in counterterrorism.***

- ***Wherever Intelligence Community leaders draw the "lanes in the road," some component must focus relentlessly and exclusively on developing all leads that can point to the US homeland.***

- ***To increase seamlessness throughout the intelligence and law enforcement communities, agencies should increase the rotation of officers among these organizations. (U)***

A fourth area isolated by the panel and requiring urgent attention is the confusion that exists in the Community around how to handle US Persons data. This accounted for numerous missed opportunities relating to Aulaqi and Hasan—both US Persons—and for these types of cases represents a

problem approximating in seriousness the shortfalls we document on information technology. (U)

We saw a surprising level of disagreement, even among experienced experts, on whether current authorities allow intelligence collectors, analysts, and law enforcement personnel to seamlessly track terrorists who communicate with US Persons or who land on US soil and thus acquire US Person status. Officers in various agencies expressed everything from unease to worry about inadvertent mistakes to fear of professional rebuke if they strayed outside existing guidelines. In many cases, the panel sensed that officers had the authority they needed but were erring on the side of caution—a subtle form of risk aversion. (U)

These tendencies had practical and worrisome consequences in the two cases we studied. [redacted]

(b)(1) (b)(3) NSA

(b)(1) (b)(3) ODNI

~~(TS//SI//NF)~~

Given the increased threats to the US homeland in the last year, including an increasing number originating here or involving US Persons, it takes little imagination to grasp how the next terrorist surprise could be the result of confusion or excessive caution about how to manage this issue. (U)

To summarize our recommendations in this area:

- ***The ODNI and the Department of Justice must come together to help the Community update, harmonize, simplify, and, where necessary, modify procedures for dealing with US Persons data.***

- ***The ODNI, working closely with the Department of Justice, must meet a need for standardized, continual, Community-wide training on how to address US Persons issues, making sure that agencies are aware of, and maximizing their use of, existing authorities that are designed to both protect privacy and civil liberties while enabling collection.***

- ***Such training and guidance must focus on working-level analysts and collectors—those who have to make decisions rapidly on the front lines—where delay or confusion can open up vulnerabilities or lead to lost opportunities.***

- ***The Community should engage key foreign liaison partners to develop plans to ensure collection in a way that is aggressive and timely but consistent with any protections for US Persons. (U)***

What More?

The recommendations in the above four areas cover most of what the DNI asked the panel to address in its first two tasks. Most of this can be accomplished within individual agencies or under existing DNI authorities. In thinking about the third task—what might the Community do beyond these things and what might new terrorist threats look like—the panel considered several "blue sky" ideas and tried to probe beyond current wisdom about the nature of the threat. (U)

Briefly developed in the text are some ideas along those lines, including how we might accelerate the development of improved information technology through a "Manhattan Project" approach; how we might make increased use of "matrix" management techniques to erase some of the seams in the counterterrorism community; how we might build a "Name Trace Central" to work that problem end to end; how the Intelligence Community's role in the visa issuance process could be expanded; and how the Community might further leverage the expertise of organizations such as State's Bureau of Intelligence and Research and Homeland Security's Office Intelligence and Analysis. (U)

Accomplishing most of these in a direct and efficient manner would involve substantial disruptions and probably would strain DNI authorities as currently formulated and exercised. (U)

Looking to the issue of how terrorism is evolving, the panel absorbed some sobering messages from the experts it separately convened from inside and outside the Intelligence Community. The key ideas that emerged strengthened the panel's conviction that the Community must prepare for more challenging days ahead. According to these experts, among the things the United States must anticipate are:

- [redacted] (b)(1) (b)(3) CIA

- [redacted]
- [redacted]

(b)(1)
(b)(3)
CIA

- A growing need to focus more intently on the people and networks that enable disaffected individuals such as Abdulmutallab or Aulaqi to become operational.

- The need for a well-developed model of the radicalization process from which the Community can derive indicators of an individual's propensity to adopt violent tactics. We have a strategic template for understanding foreign-based threats. We do not have a widely understood one for the homeland. ~~(S//NF)~~

While we have concentrated our review on the Intelligence Community, the panel comes away convinced that preventing the next Abdulmutallab-like attempt—or any counterterrorism effort more broadly—requires focusing on more than just the Intelligence Community: law enforcement, airport security, the policy community, foreign partners, and even the private sector need to address the systemic weaknesses that made Fort Hood and the 25 December incidents possible. At the risk of falling back on a cliché, we are reminded of the axiom that a chain is only as strong as its weakest link. Improved collection will not matter without sound analysis. Sound analysis will not matter without a robust watchlisting system. A robust watchlisting system will not matter without effective airport screening technology. Better screening technology will not matter without skilled screeners. There are multiple variations one could make on this chain of events, such as the vital role of foreign screeners at airports abroad—but all would reinforce the same point: the Intelligence Community is only one of several layers of our homeland security defense. (U)

To finally defeat terrorism requires at least three things: destroying the leadership, denying it safehaven, and changing the myriad conditions that give rise to the phenomenon. *The Intelligence Community can carry much of the burden on the first two—but very little on the third.* (U)

Finally, constancy of support for, and policy regarding, the Intelligence Community is crucial. While intelligence stands apart from politics, policy

toward it is forged in a political environment. We cannot emphasize enough that the pendulum swings and ebbing and flowing of support is an obstacle to mission performance. NCTC, for example, was slated to lose roughly 35 positions prior to Christmas. The post-Christmas reaction to Flight 253 has caused the number of watchlisting nominations to skyrocket; warning has become so common that the Community risks creating its own "signals-to-noise" problem. We have seen the same pendulum swings on the collection side, where agencies—acutely aware of past controversies—have erred on the side of caution, sometimes unnecessarily slowing the dissemination of valuable intelligence. The Community's Congressional overseers have a vital role to play in helping to stabilize counterterrorism policies and keep them on a steady course. (U)

Contents

Appendix

Scope Note (U)

On 15 January 2010, Dennis C. Blair, Director of National Intelligence, established the Intelligence Community Review Panel (ICRP) to explore the role and performance of the Intelligence Community leading up to and immediately following the November 2009 shootings at Fort Hood, Texas, and the attempted bombing of Northwest Flight 253 on 25 December. Specifically, the DNI charged the review group with three tasks:

- providing a detailed factual recounting of those events, to include what information was available to the Community and what was done with it;
- providing a review of what went wrong in the Intelligence Community's performance and assessing the various recommendations and corrective actions that other review groups have already put forward for discussion;[2]
- and offering an assessment of improvements that other review groups may have overlooked and that we judge could reduce the likelihood of future incidents such as Fort Hood and Flight 253. (U//~~FOUO~~)

Between 15 January 2010 and 15 April 2010, panel members and staff reviewed hundreds of documents related to the incidents, ranging from raw intelligence to finished intelligence production and postmortem assessments conducted by multiple organizations. Members and staff conducted roughly 70 interviews, meetings, and roundtable discussions with approximately 300 key decision makers, program managers, officers, and agents from components in the Office of the Director of National Intelligence (ODNI), the National Counterterrorism Center (NCTC), the Central Intelligence Agency (CIA), including its Counterterrorism Center (CTC), the Defense Intelligence Agency's (DIA) Joint Intelligence Task Force-Counterterrorism (JITF-CT), the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), the Department of Homeland Security (DHS), the Office of the Undersecretary of Defense for Intelligence, and the National Security Council. We do not identify officers by name or title in this report unless it is essential to the credibility of our judgments. Many of the meetings included follow-up requests for information.

- We shared our draft of the factual recounting of events leading up to Fort Hood and 25 December with senior officers at CTC, NCTC, FBI, and

NSA, and solicited reactions and factual corrections. Any remaining errors are our own.

- To refine and challenge our thinking, we consulted two groups of experts—one internal and one external to the Intelligence Community—to speculate on what terrorists might consider next, and how the intelligence and law enforcement communities can anticipate those challenges. We incorporated some of their ideas in formulating our recommendations.

- Finally, we brought in four external experts to review the draft and offer comments on its logic, clarity, and recommendations. (U)

Despite our best efforts, our work remains incomplete: new information continues to arrive that refines, clarifies, or challenges our understanding of both events. We had limited access to some materials related to the Fort Hood incident, some of which undoubtedly would affect our judgments; agencies and departments varied highly in the level of detail they provided; and we had only 90 days to research and draft this report.

- We focused more on the 25 December incident because the implications and responsibilities of the Intelligence Community were greater than in the case of Fort Hood and because both the Department of Defense (DoD) and the FBI had commissioned outside reviews concerning Fort Hood. Where possible, we relied on information gathered for these and other studies, such as the ODNI 30-day review.

- FBI Headquarters asked us not to interview field agents because the Army team responsible for prosecuting Hasan indicated that these agents are possible witnesses in the military prosecution.

- Similarly, we were unable to obtain the restricted annex of the DoD Independent Review Group's report on the Fort Hood Incident, referenced in media reports discussing derogatory information on Hasan that was not included in his official DoD personnel files.[3] (U~~//FOUO)~~

It is very important to note that what follows is written in the spirit of critical, objective self-evaluation that has characterized the Intelligence Community. Our posture is one of assessing these events dispassionately and clinically, fully aware that the shortcomings are not typical of the Intelligence Community's counterterrorism performance. Our aim is simple: to develop a clear-eyed, independent understanding of what we need to improve in order to make the Community's performance even

better. And the ultimate objective we must all share is to make the adversary's task harder. (U)

Panel members were the Honorable John McLaughlin, former Deputy Director of Central Intelligence; Mr. Dale Watson, former Executive Assistant Director for Counterterrorism and Counterintellligence at the FBI, and the first FBI deputy director at the CIA's Counterterrorism Center; Dr. Peter Weinberger, a senior scientist at Google and a member of NSA's external advisory board; and Mr. Alexander Joel, an attorney serving as Civil Liberties Protection Officer in the Office of the Director of National Intelligence.

- Staff members were four senior officers with experience in the CIA's National Clandestine Service (NCS), Directorate of Intelligence, and Counterterrorism Center; the National Counterterrorism Center; and the Office of the Director of National Intelligence. (U)

Report to the Director of National Intelligence on the Fort Hood and Northwest Flight 253 Incidents (U)

(b)(1) (b)(3) (b)(7)(E) FBI

(b)(1) (b)(3) NSA

[redacted] ~~(S)~~

What Happened? (U)

On 5 November 2009, Army Major Nidal Hasan opened fire at Fort Hood, killing 13 military personnel and wounding or injuring 43 military and civilian personnel before being incapacitated by police and taken into military custody.[4] Seven weeks later, Nigerian Umar Farouk Abdulmutallab boarded Northwest Airlines Flight 253 departing Amsterdam bound for Detroit, Michigan. Abdulmutallab tried to ignite an explosive device as the plane neared Detroit, but did not fully detonate the explosive. He was quickly subdued by fellow passengers and taken into custody upon landing. (U)

What follows are factual accounts of what the intelligence and law enforcement communities did in the runup to these events. These are not intended to be exhaustive. These accounts highlight, based on available data, what the Community knew, when and how it knew it, and where the Community might have had an opportunity to affect the course of events. (U)

The Shootings at Fort Hood, Texas, 5 November 2009[b]

[redacted]

(b)(1) (b)(3) (b)(7)(E) FBI

(b)(1) (b)(3) NSA

- [redacted]

(b)(1) (b)(3) (b)(7)(E) FBI

(b)(1) (b)(3) NSA CIA

[b] For additional detail on the facts and circumstances leading up to the shootings at Fort Hood, see the DoD, FBI, and ODNI *Preliminary Review of Intelligence and Intelligence Sharing on Nidal Malik Hasan Prior to the Fort Hood Shootings*, submitted to the White House on 30 November 2009, the DoD West-Clark report, *Protecting the Force: Lessons from Fort Hood*, and the forthcoming report by Judge Webster, who is leading an independent review of the FBI's actions with respect to Fort Hood. (U)

[c] [redacted] (U)

(b)(7)(E) FBI

This assessment was prepared for the Director of National Intelligence by the Intelligence Community Review Panel. (U)

(b)(1)
(b)(3)
(b)(7)(E)
FBI
(entire
page)

(b)(1)
(b)(3)
NSA

[redacted]

- [redacted]

~~(S//OC/NF/~~

- [redacted]

(b)(1)
(b)(3)
NSA

[redacted]

- [redacted]

" ~~(S//OC/NF/~~

(b)(1)
(b)(3)
NSA

[redacted]

(b)(1)
(b)(3)
NSA

[redacted]

~~(S//OC/NF/~~

- [redacted]

(b)(1)
(b)(3)
NSA

- [redacted]

(b)(1) (b)(3) NSA

(b)(1) (b)(3) (b)(7)(E) FBI

[redacted] n.

~~(S//OC/NF/~~ [redacted]

(b)(1) (b)(3) NSA

[redacted] ~~(S//OC/NF/~~ [redacted]

On 27 May, the Washington Field Office replied to San Diego's January EC.[10] WFO's review of open source, FBI, and DoD databases had produced no derogatory information on Hasan. In fact, they discovered that Hasan had been promoted to major ten days previously and was conducting research on Islamic beliefs' impact on views of military service in Iraq and Afghanistan—research that Hasan's supervisors had praised as having "extraordinary potential to inform national policy and military strategy."

(b)(1) (b)(3) (b)(7)(E) FBI

- [redacted]

(b)(1) (b)(3) NSA

- [redacted]

Anwar al-Aulaqi's Dual Roles—Inspiring and Planning Homeland Attacks

Aulaqi is a common element in the Fort Hood and 25 December incidents. Aulaqi first came to the attention of the Intelligence Community in the wake of the 9/11 attacks because of his contacts with two of the hijackers. The Community then viewed him as a fundamentalist imam, with a mainstream following, whose lectures were being followed by English-speaking Muslims. Analysts at the time assessed he was not a member of a terrorist organization and focused largely on his growing status and influence as an ideologue. ~~(S//NF)~~

Community analysts observed Aulaqi's influence increasing among homegrown extremists after his release from a Yemeni prison circa December 2007 and the subsequent launch of his website. [redacted] At the same time, he began to propagate videos and statements to Western audiences, many of which encouraged individuals to support or participate in violent jihad. His early 2009 statement, entitled "44 Ways to Support Jihad," advocated martyrdom against the United States and financial support to mujahidin.[11] ~~(S//NF)~~

(b)(1) (b)(3) (b)(7)(E) FBI

[redacted] ~~(TS//HCS/SI/NF)~~

(b)(1) (b)(3) (b)(7)(E) FBI

(b)(1) (b)(3) NSA CIA

(b)(1)
(b)(3)
(b)(7)(E)
FBI
entire
page

(b)(1)
(b)(3)
NSA

- [redacted] ~~(S//OC/NF/~~ [redacted])

(b)(1)
(b)(3)
NSA

[redacted]

- [redacted]

- [redacted]

d [redacted] ~~(S//OC/NF/~~ e [redacted] ~~(S//NF)~~

(b)(1)
(b)(3)
NSA

[redacted] ~~(S//OC/NF/~~ [redacted]

(b)(1)
(b)(3)
NSA

[redacted] ~~(S//OC/NF/~~ [redacted]

(b)(1)
(b)(3)
NSA

[redacted] ~~(S//OC/NF/~~ [redacted]

(b)(1)
(b)(3)
NSA

[redacted] ~~(S//OC/NF/~~ [redacted]

[redacted] ~~(S//NF)~~

Fort Hood: Red Herrings and Conventional Wisdom (U)

Media coverage of the Fort Hood shootings—and comments attributed to anonymous US officials—have framed the public and political discussions of the event, but the coverage has included inaccuracies that have skewed the discussions. Some of these include:

- *Aulaqi directed Hasan's attack at Fort Hood.* There is no evidence indicating that Aulaqi directed Hasan.
- [redacted] (b)(1) (b)(3) (b)(7)(E) FBI (b)(1) (b)(3) NSA
- *FBI had access to negative information in Hasan's personnel file.* Media reports indicate that Hasan's colleagues and superiors questioned his judgment and fitness, citing his presentations and other statements. The only derogatory information in Hasan's official DoD personnel file was that he did not take a required physical fitness exam in 2008. Hasan's file was nearly uniformly positive, including praise for his scholarly work on Muslims as having "extraordinary potential to inform national policy and military strategy."
- [redacted] (b)(1) (b)(3) (b)(7)(E) FBI
- [redacted] ~~(S//OC/NF/~~[redacted]

The Attempted Bombing of NW 253, 25 December 2009

(b)(1) (b)(3) NSA

In the runup to these developments—and in the immediate aftermath—the Intelligence Community [redacted]

- [redacted]

(b)(1) (b)(3) NSA

- [redacted]

- [redacted]

(b)(1) (b)(3) NSA

- [redacted]

(b)(1) (b)(3) NSA

[redacted] ~~(TS//SI//NF)~~

(b)(1) (b)(3) NSA

[redacted] was thus unaware of the [redacted] when, approximately one week later, Abdulmutallab's brother and father—the latter a well-connected member of the Nigerian elite—met with [redacted] to relay their concerns about Umar Farouk. [redacted] he father said that he was concerned his son "had fallen under the influence of unspecified religious extremists;" had become "active in the college mosque" while studying in London; and that his son planned to "commit his life to *dawa*," or proselytizing. Abdulmutallab's family also assessed that Umar Farouk was "a victim of inexperience and naivety and influenced to join groups who would be willing to engage in illegal acts in the name of religion." ~~(S//HCS//OC/NF)~~

(b)(1) (b)(3) CIA

The father did not explicitly associate his son with terrorism and provided no names of the religious extremists.[28] The father noted that intelligence

---

[f] [redacted] ~~FS//SI//NF)~~

(b)(1) (b)(3) NSA

services [redacted] whom the father had queried, reported having no derogatory information on his son; that the son planned to stay in Yemen to study *sharia* for the next seven years; and that his son had not withdrawn funds from his bank account.[29] The father provided copies of his son's passports, date and place of birth, photographs, and biographic information [redacted]

(b)(1) (b)(3) CIA

The biographic information—including name, age, education, and travel experience—was consistent with the biographic information and partial name in the [redacted] that had not reached [redacted][30] ~~(S//HCS//OC/NF)~~

(b)(1) (b)(3) NSA

[redacted] CIA Headquarters to conduct name and phone number traces on the son and add him to the terrorist watchlist. [redacted][g]

(b)(1) (b)(3) CIA

- [redacted] its name trace on Abdulmutallab was conducted in a system that contained only CIA traffic, and found no hits.[31]

(b)(1) (b)(3) NSA CIA

- [redacted] CTC watchlisting advises subject does not currently meet the threshold for terrorist watchlisting. In order to place subject on a watchlist, there needs to be some indication of involvement with attack planning, joining a terrorist group, providing material support to known/suspected terrorists, or desire to become a martyr/suicide bomber."[32] [redacted]

(b)(1) (b)(3) CIA

- As we discuss elsewhere, the draft intelligence report was not disseminated until after the incident on 25 December. ~~(S//HCS//OC/NF)~~

[redacted] place a 'look out' for Umar Farouk Abdulmutallab in the State Department Consular Class System," the State Department's visa database.[33] The Embassy, in turn, sent a Visas Viper cable addressed to State/INR, NCTC, FBI, and DHS—notifying them about Abdulmutallab's possible ties to extremists.

(b)(1) (b)(3) CIA

- State Department's Visas Viper cable prompted NCTC to create a record for Abdulmutallab in NCTC's Terrorist Information Datamart Environment (TIDE).

- [redacted] searched the State Department's visa and immigration databases, but because the State officer misspelled "Abdulmutallab," did not use a name variant search tool, and did not search on his passport number, the search did not flag that Abdulmutallab held an active US visa, which could have caused officers to focus more on him.[34]

(b)(1) (b)(3) CIA

- Recognition that Abdulmutallab held a US visa would not, however, have automatically triggered a specific procedural step, such as placement on the No Fly or Selectee list.

- [redacted] ~~(S//HCS/OC/NF)~~

(b)(1) (b)(3) CIA

---

g [redacted] ~~(S//NF)~~

(b)(1) (b)(3) CIA

(b)(1) (b)(3) NSA

The Intelligence Community received a handful of reports over the next several weeks that, in retrospect, almost certainly pertained to Umar Farouk Abdulmutallab. [redacted][37]

(b)(1) (b)(3) NSA

- [redacted] NCTC highlighted the report in a 1 December interagency secure videoteleconference, and NCTC officers wrote about the report for policymakers in a 10 December DNI Homeland Task Force Update.[38] ~~(TS//SI//NF)~~

Strategic Warning and Threats to the Homeland (U)

The Intelligence Community was focusing on the threat posed by AQAP well before the events of 25 December, although as recently as October 2009 there were disagreements about its intent and capability to take on anti-homeland operations. The Community had long followed Aulaqi, who was mentioned in the 9/11 Commission Report.[39] NCTC's Fiscal Year 2010 Counterterrorism Production Guidance placed emphasis on the growing challenge posed by al-Qa'ida's presence in the Horn of Africa.[40]

(b)(1) (b)(3) CIA

- [redacted]

(b)(1) (b)(3) NSA CIA

- An October 2009 "Memo to the Holders" of a 2007 NIE produced by the National Intelligence Council starkly warned about the threat posed by Yemen-based jihadists and the fact that their access to dual Yemeni-US citizens strengthened their capabilities. Nonetheless, the majority assessed with high confidence that al-Qa'ida would have limited success mobilizing affiliates to attack the homeland. [redacted][42]

(b)(1) (b)(3) CIA

- [redacted] ~~(S//NF)~~

(b)(1) (b)(3) NSA

Much of the all-source analysis was made possible by increasingly robust collection. [redacted] ~~/NF)~~

(b)(1) (b)(3) NSA

[redacted] ~~(TS//SI//NF)~~

(b)(1) (b)(3) NSA

[redacted]

- [redacted]
- [redacted]

(b)(1) (b)(3) NSA

- [redacted] ~~(TS//SI//OC/NF)~~

On 25 December, Abdulmutallab entered the Schiphol Airport in Amsterdam. Dutch authorities pulled him aside for secondary screening because of immigration concerns; TSA officers whom we interviewed said that Abdulmutallab revealed no signs of nervousness during the screening; airport screeners x-rayed his carry-on luggage and directed him through a standard metal detector without incident. Passengers seated near Abdulmutallab later told US investigators that he demonstrated no unusual behavior until the incident.

- As the flight neared landing, Abdulmutallab tried to ignite a chemically detonated explosive; the device did not ignite properly, and Umar Farouk was subdued by other passengers. The Intelligence Community learned during subsequent debriefings that Abdulmutallab had received unspecified training from explosives expert Ibrahim Hasan Asiri, who had been connected to the attempted assassination of Saudi Minister of Interior Prince Mohammed bin Nayif. Asiri had provided Abdulmutallab with modified pants and syringes, with the goal of taking down an aircraft over US soil.

(b)(1) (b)(3) CIA

- After Abdulmutallab was arrested, [redacted] formally disseminated the [redacted] intelligence report, at which point [redacted] saw the intelligence report for the first time.[47] ~~(S//NF)~~

(b)(3) NSA

NW 253: Red Herrings and Conventional Wisdom (U)

Media coverage of the 25 December attempted bombing—and comments attributed to anonymous US officials—have framed the public and political discussions of the event, but the coverage has included inaccuracies that have skewed the discussions. Among the errors:

- *Abdulmutallab's father warned that his son was likely to commit a terrorist act.* Dailies and major networks have reported that the father warned that his son "had been in contact with Muslim terrorists and that his son had met with militants in Yemen;"[48] that his son "had been in contact with Muslim terrorists;"[49] that "his son was a potential terrorist" who was "planning an attack;"[50] that Abdulmutallab had "volunteered for terrorist operations;"[51] and that his son had "ties to suspected al-Qa'ida operatives in Yemen."[52] In fact, the father had said that his son "had fallen under the influence of unspecified religious extremists," proffered no connection to terrorism, and provided no hints of martyrdom or affiliation with al-Qa'ida.[53]

- *The State Department's misspelling of Abdulmutallab's name allowed him to obtain a visa.*[54] In fact, Abdulmutallab received a multi-entry US visa in June 2008 that was valid until 2010.

- *Abdulmutallab purchased a one-way ticket, in cash, and brought no luggage on his trip, which should have raised authorities' suspicions.*[55] Abdulmutallab did in fact pay cash for his ticket, though the purchase was not extraordinary in cash-based countries suffering double-digit inflation.[56] Contrary to press reports, Umar Farouk had purchased a roundtrip ticket and brought carry-on luggage with him.[57]

- *Abdulmutallab sailed through airport screening.*[58] Abdulmutallab received additional scrutiny from Dutch authorities in Amsterdam, who were concerned about potential immigration fraud; he passed through a metal detector and his carry-on luggage was x-rayed. TSA officials told us that it remains inconclusive whether state-of-the-art airport screening technologies would have detected the trace amounts of chemicals positioned on Abdulmutallab's body.

- *The US Government did not know that Abdulmutallab was aboard the flight until after the plane departed Amsterdam.*[59] Customs and Border Protection (CBP) received the full passenger list before takeoff and compared it against a database looking for matches with the No-Fly and Selectee lists, neither of which included Abdulmutallab. Further screening of the passenger list uncovered an entry on Abdulmutallab based on the State Department's Visas Viper cable, which is why CBP officers—before the incident—had decided to interview Abdulmutallab upon arrival.

- *The Community did not realize that Aulaqi was a common thread in the Fort Hood shootings and the 25 December attack.*[60] [redacted] the Community had noted his emergence as an operational planner in May 2009.[61] [redacted] (b)(1) (b)(3) (b)(7)(E) FBI (b)(1) (b)(3) NSA

- *The Intelligence Community did not know that AQAP had the intent to launch an attack against the homeland.*[62] An October 2009 "Memo to the Holders" included a warning [redacted] that jihadist networks on the Arabian Peninsula and in East Africa were following al-Qa'ida's anti-US global agenda and had the capabilities to plot operations against the homeland.[63] ~~(TS//HCS/SI//OC/NF)~~ [redacted] (b)(1) (b)(3) NSA

(b)(7)(E) FBI (b)(1) (b)(3) CIA

Some Preliminary Thoughts on Learning from These Incidents (U)

In assessing the events recounted above, the panel believes it is important to keep in mind the following three points. (U)

First, there is no recipe for perfection. Terrorists will not stop trying to penetrate our defenses, and some are going to get through. The American public, elected leaders, and Intelligence Community officers are understandably uncomfortable with that idea, but it is an unavoidable reality—one that should be communicated to the American people. The task of identifying and screening terrorists who may seek to travel to the United States is a daunting one, and illustrates the signals-to-noise challenge. More than 1.2 million travelers try to enter the United States by air, land, and sea every day. Consider the scope of the air travel problem: passengers enter from 245 airports on more than 1,600 flights each day; TSA officers screen 1.8 million travelers entering and departing US airports across the country each day.[64] No amount of collection, no aggregation of data, and no level of information technology will guarantee the government detects and prevents all terrorists from making it onto US-bound aircraft or into the United States.

- Worse yet, the United States is dealing with a nimble adversary that constantly adjusts to exploit any weak link in the homeland security system. Better US collection capabilities prompt terrorists to adopt newer and more exotic forms of communications; more invasive airport screening technologies prompt terrorist to seek new ways to evade screening—such as entering through countries where patdowns are taboo—or alternative modes of entry, such as by sea or by land. Every US success is a learning opportunity for terrorists.

- Individuals already inside the United States, who decide to use violence to pursue the aims of foreign terrorist groups, pose another threat with unique challenges to detection and prevention—particularly if they limit travel abroad and communication with known terrorist groups. If we are to identify "homegrown extremists," we must develop new methods to detect threats in the homeland, consistent with our laws and respect for civil liberties, and enlist the support of all Americans. Here, too, there are no guarantees. ~~(C//NF)~~

Second, information overload has made the signal-to-noise challenge even harder in recent years. The intelligence, homeland security, and law enforcement communities are swimming in data and often armed with outdated information technology; more analysts are needed to cover some of the nation's most critical national security challenges. Our recommendations address these areas, together with changes in work processes that must accompany them. The Community must recognize, however, that additional resources and better technology—while necessary and welcome—are no panacea. More information will always be available to be analyzed and correlated. These changes can only reduce—not eliminate—risk. (U)

Third, in assessing the events leading up to both incidents, and in considering any set of changes to the counterterrorism community, it is important to remember that choices will entail tradeoffs—fiscal, bureaucratic, and so on. Ultimately, where to draw the line on those issues is a political decision, but the entire Washington community should understand that choices will have potentially unpopular—and almost certainly unintended—consequences.

- Surging analysts to cover an emerging threat means moving analysts off other accounts, which risks creating gaps on other threats. [redacted] (b)(1) (b)(3) NSA CIA

- Easing standards to place more suspected terrorists on the No Fly/Selectee lists carries clear tradeoffs, such as a likely surge in false positives. Allowing collectors to nominate suspected terrorists on partial names—increasing the likelihood of detecting their travel—risks compromising collection programs

when individuals are linked with aliases used only in their covert communications, while better information sharing with foreign governments or the airline industry increases the risk of compromising sensitive information.

- Requiring the airline industry to do more to support the Intelligence Community—such as sharing passenger lists earlier than 30 minutes before takeoff—could require earlier check-in times for travelers, undoubtedly an unpopular move.[65] Requiring that airline companies inform the US Government whenever an individual on the No-Fly List tries to purchase a ticket probably would meet with complaints that the US Government is imposing costly additional burdens on the industry.

- Instituting a minimum waiting period to acquire a US visa, which would give State Department and the Community more time to research suspicious applicants, would undoubtedly prompt complaints and perhaps even in-kind retaliation from some foreign governments. ~~(S//NF)~~

Missed Opportunities: The Context and the Consequences (U)

As the panel reflected on these events, we were acutely aware that hindsight always brings greater clarity. We also readily concede that our judgments are in some ways provisional, because new information will probably emerge in the coming months. We learned this lesson in our review, when the government in February obtained [redacted] that challenged some of our own thinking. Still, three points stand out:

(b)(1) (b)(3) NSA

- These events did not occur in a vacuum; the operational tempo and workflow for the Intelligence Community were heavy and sustained throughout 2009 and in the lead-up to both incidents. Both cases had novel aspects not previously seen by the Intelligence Community; the 25 December incident was the first attack against the homeland by an al-Qa'ida affiliate.

- Nonetheless, the intelligence reporting that could have led the Community to identify Umar Farouk as a potential terrorist threat before 25 December merited greater scrutiny—although Intelligence Community follow-up actions would not have necessarily have kept him off the airplane.

- Causes of these "missed opportunities" ranged from human error to poor decisionmaking; heavy work volume; an occasional lack of individual inquisitiveness or understanding about who was responsible for driving an issue through to its resolution; ambiguous roles and responsibilities; a lack of understanding of key databases; and information technology systems that do little to help officers and agents find and correlate key bits of reporting amidst a sea of data. ~~(TS//SI//NF)~~

During our review, we were consistently impressed by the pace, scope, breadth, and depth of the Community's counterterrorism efforts throughout 2009, many of which produced notable successes.[h] During this period, analysts were tracking multiple threats or supporting operations to counter them: [redacted] fielding multiple requests for briefings; producing a steady stream of current production; participating in daily teleconferences with collectors, policymakers, and the law enforcement community; and providing analysis and support following the June shootings at a US military

(b)(1) (b)(3) NSA CIA

[h] NCTC's *Homeland Year in Review for 2009* noted, "Successful attacks, disrupted plots, and arrests of Sunni extremists in the US in 2009 reached their most significant level since 2001." ~~(S//NF)~~

recruiting center in Little Rock, Arkansas.[66] We discuss further some of the successes we encountered in the course of our review, and ways in which success can create new challenges for the Community, in Appendix B. ~~(TS//HCS/SI//NF)~~

In addition to these other pressures, counterterrorism officers were working with enormous data flows:

(b)(1) (b)(3) NSA CIA

- [redacted]

(b)(1) (b)(3) (b)(7)(E) FBI

(b)(1) (b)(3) NSA

- [redacted]

- Moreover, the 25 December attack developed in a compressed timeframe, unlike the methods of plotting typically used by al-Qa'ida. ~~(TS//HCS/SI//OC/NF/~~[redacted]) (b)(7)(E) FBI

It is thus too simple to call this a "connect the dots" problem—a metaphor that strips away context and trivializes the challenge counterterrorism officers face in dealing with massive volumes of data. The 25 December case in particular is more akin to what scholar Roberta Wohlstetter in her classic study of Pearl Harbor called the "signals to noise" problem.[68] In short, the fragmentary clues about Umar Farouk's plans—the "signals"—were deeply submerged in a vast pool of intelligence reporting—thousands of messages a day, the "noise." The task then, and the North Star guiding this panel's efforts, has been the question of how to raise such alarming "signals" from a body of noise that is growing rapidly as technology enables both the creation of more data and the Intelligence Community's ability to collect it. ~~(S//NF)~~

But even allowing for a challenging "signals to noise" ratio, the panel could not avoid concluding that the body of reporting related to the 25 December case deserved greater attention than it received. To be sure, hindsight separates the "signals" from the "noise" in a way that was far more difficult at the time. [redacted] (b)(1) (b)(3) NSA was not surprising given that Nigeria is the world's eighth most populous country. That context is essential. ~~(TS//SI//NF)~~

What moved the panel to the view that this case should have stood out from the noise was not just the combined weight of [redacted] ***an especially ominous report on 30 November,*** [redacted] (b)(1) (b)(3) NSA (b)(1) (b)(3) CIA Competing priorities, information overload, cumbersome technical tools—all were factors that help explain why many of these reports were not actively pursued. "Stovepiping" of accounts, however, was not—these reports were sufficient to raise red flags for analysts covering AQAP operatives, AQAP use of foreigners, AQAP travel plans, or AQAP threats against the homeland. We highlight below the opportunities for this case to surface:

- [redacted] (b)(1) (b)(3) NSA

(b)(1) (b)(3) NSA

- [redacted]

- Sorting out reasons why these reports did not receive more attention led us to conclude that either they were submerged in a heavy volume of reporting or simply reinforced analysts' concerns about the threat posed by Aulaqi and AQAP to targets inside Yemen—a danger to which the Intelligence Community already was alert and acting on.

(b)(1) (b)(3) NSA

(b)(1) (b)(3) CIA

- [redacted]

(b)(1) (b)(3) NSA

(b)(1) (b)(3) CIA

- [redacted]

(b)(1) (b)(3) CIA

(b)(1) (b)(3) NSA

- A fourth opportunity [redacted] describing Umar Farouk Abdulmutallab, whose biographic information—including name, age, education, and travel experience (e.g., Yemen)—matched that of the "Umar Farouq," last name unspecified, identified in [redacted] ~~(TS//HCS/SI//OC/NF)~~

The panel identified one report that should have prompted robust pursuit by the Intelligence Community and could have led to identification of Umar Farouk Abdulmutallab as a potential threat before 25 December. But—emblematic of the challenges facing counterterrorism officers—this report included no biographic data for the unnamed associate who, in retrospect, almost certainly is identifiable with Umar Farouk Abdulmutallab.

(b)(1) (b)(3) NSA

- [redacted]

(b)(1) (b)(3) ODNI

(b)(1) (b)(3) CIA

- [redacted] This threat may have received more attention if it had been linked [redacted]

- We cannot rule out that there were efforts to pursue this thread that the panel did not uncover. But we were unable to document any follow-up. Short of a scrub of known AQAP operatives or an intensive

(b)(1) (b)(3) CIA

and creative search of cable traffic, uncovering Abdulmutallab—or any other affiliate of AQAP with a passport or visa that would enable travel to the United States or UK—would have required sophisticated data manipulation [redacted] ~~(TS//SI//NF)~~

(b)(1) (b)(3) (b)(7)(E) FBI

[redacted]

- [redacted]

(b)(1) (b)(3) FBI

- [redacted]

(b)(1) (b)(3) FBI

- [redacted]

(b)(1) (b)(3) FBI

[redacted]

(b)(1) (b)(3) FBI

- [redacted] ~~S//OC/NF~~ [redacted]

(b)(1) (b)(3) (b)(7)(E) FBI

The panel recognizes that these recitations alone—in which we isolate reports and lay them out serially—makes detection and warning of terrorism sound easier than it is. We have no illusion that this neat overview approximates in any way the real world of the Community's counterterrorism analysts and law enforcement counterparts. But we do think it was *possible* to make these connections. In much of what we recommend, we discuss strategies intended to make that *more likely* to occur in the world of heavy reporting volumes, competing demands, and high operational tempo that terrorism analysts actually occupy. (U//~~FOUO~~)

There were several missed opportunities that could have increased the odds of detecting Abdulmutallab or Hasan. The causes of the missteps ranged from human error to inadequate information technology, inefficient processes, unclear roles and responsibilities, and an occasional lack of individual inquisitiveness.

- *Several key reports did not reach people who might have acted on them.* [redacted] coupled with the fact that CIA did not disseminate [redacted] before 25 December, prevented officers [redacted] from piecing together two key reports.

(b)(1) (b)(3) NSA CIA

- We believe the details in each report were so similar that someone [redacted] would have made the connection. [redacted] e would have

(b)(1) (b)(3) NSA

(b)(1) (b)(3) NSA

[redacted] At a minimum, it would have allowed analysts to search other reporting databases—and even the blog postings on the Internet—for derogatory information on Abdulmutallab.[79]

(b)(1) (b)(3) NSA

- [redacted]

(b)(1) (b)(3) NSA CIA

- [redacted]

- *Name trace processes were inadequate.* [redacted]

(b)(1) (b)(3) NSA CIA

(b)(1) (b)(3) (b)(7)(E) FBI

- *State Department's errant name trace did not reveal that Abdulmutallab had an active US visa,* which could have raised the Community's attention. Moreover, no one apparently noticed that Abdulmutallab's passport from several years earlier indicated that he had a pending visa application in 2008.

(b)(1) (b)(3) (b)(7)(E) FBI

(b)(1) (b)(3) NSA

- [redacted] ~~(TS//SI//HCS//OC/NF~~[redacted]

In both cases, the inadequacy of information technology for aggregating and correlating the relevant reporting was striking. To be sure, much of the intelligence that could have caused Umar Farouk and Hasan to rise above the thousands of pieces of raw intelligence was available in one dataset or another; more focused searches—such as on "Umar Farouk" and "Nigeria"—would have winnowed the reporting to a manageable number. Better information technology could have helped compensate for human errors, time pressures, heavy workload, or shortcomings.

(b)(1) (b)(3) NSA CIA

- [redacted]

- Multiple officers in CTC and NCTC noted the proliferation of databases and the time-consuming nature of mastering and searching each one. JTTF personnel in WFO, for example, had to work with nearly two dozen separate databases—including one using an antiquated DOS-based system. ~~(S//NF)~~

Throughout both cases, we also observed a less tangible but equally important problem with "issue

ownership"—a lack of initiative or understanding about who was responsible for driving an issue through to its completion—which also contributed to missed opportunities.

(b)(1) (b)(3) CIA

- [redacted]

- This prompted CIA to change how it disseminates intelligence, which we detail later in this report.

- We found that counterterrorism officers from multiple agencies had widely varying degrees of familiarity with watchlisting terminology and processes in their own agency, let alone the greater enterprise, which translated into uncertainty over who had responsibility for ensuring that a suspected terrorist was placed on a watchlist.

(b)(1) (b)(3) NSA CIA

- [redacted]—but the dissemination errors were still unresolved when the key [redacted] was disseminated four months later.

- In the course of our discussions, several officers told us that a search on the name "Umar Farouk" [redacted] would have generated an unwieldy number of results because it was such a common name. [redacted] a slightly more focused search would have returned a more manageable number of results. [redacted] could have enabled CTC, NCTC, or NCS officers to tie together the reporting.

(b)(1) (b)(3) NSA CIA

- [redacted]

(b)(1) (b)(3) (b)(7)(E) FBI

(b)(1) (b)(3) NSA CIA

- [redacted] ~~(TS//SI//OC/NF/[redacted])~~

(b)(1) (b)(3) (b)(7)(E) FBI

[redacted]

(b)(1) (b)(3) (b)(7)(E) FBI

[redacted] ~~(TS//SI//OC/NF)~~ [redacted] ~~(S//NF)~~

(b)(1) (b)(3) (b)(7)(E) FBI

(b)(1) (b)(3) NSA

(b)(1)
(b)(3)
(b)(7)(E)
FBI

[redacted]

- [redacted]

(b)(1)
(b)(3)
(b)(7)(E)
FBI

- [redacted]. ~~(S//OC/NF/~~[redacted]

To summarize our conclusions on missed opportunities in these two cases:

- *The pace, scope, depth, and intensity of the Community's workload in the run-up to both events played a role in officers not treating the reporting with the sense of urgency it deserved;*

- *Inadequate information technology did not help analysts and agents aggregate and correlate relevant reporting, either because the intelligence was buried in a sea of data or spread among a maze of unconnected databases;*

- *A series of missteps ranging from human error to unclear name traces and dissemination procedures meant that key reports or information did not reach people who might have pieced them together or acted on them;*

- *Highly segmented, stovepiped processes and organizational units meant that no single entity owned either issue from start to finish—and handoff from one organization from another was often weak.* ~~(C//NF)~~

Should Abdulmutallab Have Been Prevented From Boarding Northwest Flight 253? (U)

We encountered strongly competing views on whether Abdulmutallab should have been allowed to board Flight 253. After studying the issue for 90 days and meeting with officers from multiple agencies, this retrospective question remains the closest of analytic calls. *We believe that Umar Farouk Abdulmutallab should have been nominated for watchlisting; we are less confident that the nomination would have been accepted.* ~~(C//NF)~~

(b)(1) (b)(3) CIA

CTC and NCTC judge that Abdulmutallab did not meet No Fly criteria and at best would have made Selectee status. They noted, [redacted], that Abdulmutallab's father alleged only that he was associating with unnamed "religious extremists" and that TSC's nomination guidelines at the time specifically state that "individuals described as militants, extremists, jihadists, etc., should *not* be nominated without particularized derogatory information that leads to reasonable suspicion of the individual's involvement in terrorist activity."[88] [emphasis added] Assessing combined information from both [redacted] CTC and NCTC analysts claim that TSC would not have placed Abdulmutallab on the No Fly list. ~~(S//HCS//NF)~~

(b)(1) (b)(3) NSA

TSC officers dispute that view. They agree that [redacted] did not provide sufficient derogatory information, but believe that all of the available intelligence—[redacted]—collectively provided a specific name, date and place of birth, a connection to AQAP leadership, and plans to get terrorist training. When combined, they argue, those reports met the No Fly criteria of "particularized derogatory information," and "operationally capable" intent. ~~(C//NF)~~

(b)(1) (b)(3) CIA

On balance, the panel believes that the reporting available at the time was sufficient to nominate Umar Farouk Abdulmutallab for the No Fly list; we are less confident that the nomination would have actually resulted in his placement on the No Fly list. ~~(C//NF)~~

CTC and NCTC officers noted in our interviews that TSC had recently rejected or downgraded nominations under the "operationally capable" criterion that were based on substantially more specific—and ominous—threat reporting.[k 89] We reviewed some of those examples and agree with the analysts' characterization. TSC, on the other hand, could point to No Fly nominations that were accepted on the basis of levels of specificity similar to those of the Abdulmutallab case. Proponents of both views can cite compelling examples; we could not gain access to enough information to systematically adjudicate each claim. ~~(S//NF)~~

During our interviews, we also came away convinced that the watchlisting process is only one means by which the US Government can prevent a suspected terrorist from entering the United States. If the Community had tied together the relevant reporting, [redacted] the Community might have garnered more information about his location and intent. It was not until after 25 December, for example, that his brother told US officials that Abdulmutallab had previously said that his family would never hear from him again. ~~(S//HCS//NF)~~

(b)(1) (b)(3) CIA

A final opportunity to keep Abdulmutallab off the flight would have been through enhanced airport screening, although we are skeptical that this step would have been sufficient. Dutch authorities did in fact screen Abdulmutallab during check-in because of immigration concerns, his carry-on luggage was x-rayed, and Abdulmutallab had traveled to the United States previously without incident, eliminating a potential selector of concern. It remains inconclusive whether even the state of-the-art screening technologies or invasive patdowns would have detected the chemicals because of their placement, size, and shape. At most, we believe sustained questioning could have provoked or detected signs of nervousness or inconsistent responses. ~~(S//NF)~~

---

[k] During this approximate timeframe, TSC rejected a broad range of NCTC "No Fly" requests, including several where NCTC could cite specific derogatory information. [redacted] In each case, TSC either downgraded the nominee or removed them from the No Fly list. ~~(S//NF)~~

(b)(1) (b)(3) CIA

Analysis and Recommendations on the Way Ahead (U)

As part of the panel's second task, we were asked to comment on the various recommendations that the Intelligence Community is considering—as well as those recommended by the Senate Select Committee on Intelligence (SSCI) and various nongovernment organizations—and to offer additional recommendations of our own. We do so fully aware that there will always be risks of additional incidents such as those at Fort Hood and threats to aviation security; no set of recommendations, even if fully implemented, will eliminate such recurrences. Still, we believe that many of these recommendations will increase the odds that US and foreign governments can stop similar incidents.[90]

- We found that agencies have "gone to school" on these cases and are implementing changes designed to limit chances for recurrence. We are acutely aware that as we have studied the situation and considered recommendations, a host of other agencies and the ODNI are doing the same thing simultaneously. We thus concluded that our comparative advantage lies in looking strategically across these initiatives and recommending which ones deserve added emphasis and noting where there may be gaps.

- We therefore intentionally focus on only a small segment of the actions and recommendations currently under discussion. In reviewing the after-action reports of individual agencies and units, we identified more than 100 separate proposals—some Community-wide, some specific to individual organizations—so we comment only on those that struck us as most relevant. We also flag several proposals that struck us as unwise investments of time, energy, and resources.

- Some of our recommendations are broad and long-term—and may even require legislative action; others are narrow, technical, and agency specific, but struck us as important enough to merit attention.

- We are commenting on moving targets; some initiatives are already underway.

- We also realize that some of our recommendations are not new. In part, we flag those issues for that very reason: years of interagency discussions and meetings have not produced action, even as the terrorist threat continues. (U//~~FOUO~~)

Distilling the myriad factors complicating mission performance to a manageable number, we focused our recommendations on four key areas, all of which were at play to one degree or another in the cases of either Hasan or Abdulmutallab:

- **More efficient internal processes** that help analysts locate, retrieve, and disseminate terrorism-related intelligence—and a new business practices for how the Community uses that intelligence once it has been identified.

- **An information technology infrastructure** that reduces rather than contributes to the signals-to-noise problems we have already discussed.

- **A structural division of labor** that focuses substantially greater attention and resources on threats to the homeland and plays to the comparative advantage of various Community partners.

- **Simplifying complications surrounding US Persons data**, ranging from collecting to analyzing, storing, and sharing this intelligence. (U//~~FOUO~~)

Internal Processes that Help Find Terrorists in the Data

Early in our review we identified several problems that complicate the Community's ability to "find the terrorists" in the available data. There are two components to this problem: agency-specific processes that affect the Community's access to timely, accurate information, and how that intelligence is pulled together to support the watchlisting process. The former changes are generally fixable; the latter require changing how

intelligence officers conceptualize and leverage the watchlisting process. (U)

Many of the problems we identified early were similar to those other review groups have noted. Among the earliest judgments we reached:

(b)(1) (b)(3) CIA

- NCS intelligence reports—[redacted] must be disseminated more rapidly;
- NSA field dissemination lists need to be updated;
- State Department visa searches must be more rigorous and technologically sophisticated;
- NCS names traces must be conducted in all-source databases. (U~~//FOUO)~~

We were heartened to learn that agencies have already made headway on virtually all of these issues.

(b)(1) (b)(3) NSA

- The Director of CIA has already ordered that all NCS counterterrorism-related field reports be disseminated within 48 hours of receipt, and NSA has taken steps to ensure that dissemination lists [redacted] are being scrubbed to prevent similar recurrences [redacted][91]

(b)(1) (b)(3) CIA

- [redacted]
- [redacted]
- State Department has addressed processes for conducting name traces. State Department could have searched on Abdulmutallab's passport number, which would have been more precise than a transliteration of a foreign name, and could have used a "fuzzy logic" function that could have corrected for the typographical error, but did not. In response, State Department has instructed its officers to search the Consular Consolidated Database using the "fuzzy logic" function, include all current and past visa information on the Visas Viper cable, and conduct searches on passport numbers. If implemented, these measures will increase the odds that known or suspected terrorists will be detected earlier in the visa application process.[92] ~~(S//NF)~~

We offer several additional recommendations as the Community moves forward in improving the search for terrorist identities.[93]

- Some of the steps outlined above should be expanded throughout the Community. All agencies should promptly disseminate counterterrorism reporting, update their dissemination lists on a regular basis, and conduct name traces against all of their holdings. Dissemination lists for counterterrorism-related intelligence and State Department Visas Viper cables also should be updated on a regular basis to ensure that collectors in the field receive reports germane to their area of responsibility.
- We recommend that agencies examine whether complicated dissemination codes can be standardized or simplified. The routing error of the [redacted] is a predictable consequence of having such detailed dissemination codes.

(b)(1) (b)(3) NSA

- The search for terrorist identities should be conducted against all holdings available to that agency.
- A "fuzzy logic" tool that automatically formats and searches variant spellings and renderings of foreign names, should be available and used in name traces.
- "Discoverability" should be part of the process. In practice, this means that if an all-source search

against a name or identity leads to information (such as a phone number) to which the searching officer does not have normal access, a notation will direct the officer to a point of contact who can grant access to that information.

- Officers performing identity searches should be trained to look for partial names, along with salient points such as the person's location, affiliations, passport numbers, schooling, or travel—details that can further narrow the search and identify an individual. ~~(C//NF)~~

The second half of improving the search for terrorist identities centers on the equally important issue of watchlisting—how analysts use and collate the raw reporting to identify a potential terrorist and prevent him from entering the United States. Watchlisting procedures clearly have improved over the years. Prior to 9/11, the US Government maintained 13 separate watchlists; today there is one. Since 9/11, multiple agencies transferred information from their systems into TIDE. In no way do we mean to detract from the progress to date. (U//~~FOUO~~)

Still, the panel believes that the watchlisting process needs adjustment. The Community's understanding of watchlisting is inconsistent, between and often within organizations. The nature of watchlisting—an end-to-end process spanning multiple units and organizations—has led to a segmentation and redundancy to an extent that ensures that no single individual or entity has full responsibility for a particular nomination. We saw this dynamic glaringly in the case of Abdulmutallab. It is only a matter of time before similar instances occur. (U//~~FOUO~~)

In short, individual components, even when performing their tasks efficiently and energetically, take a fairly narrow view of their roles. Everyone works very hard at it, but we were struck by the uncertainty about roles, responsibilities, and procedures. Within the NCS, we found uncertainty among officers dealing with the Abdulmutallab case about the steps in the watchlisting process, limited awareness of what analytic efforts were required to search and tie together information to formulate a watchlist request, and what CTC Watchlisting officers would do with the request; CTC Watchlisting officers assume area division officers have already searched for derogatory information and made pertinent associations before submitting the nomination, and that the job of CTC Watchlisting was to format nomination packages for passage to NCTC Watchlisting. NCTC Watchlisting officers, in turn, stressed that their primary role is entering data into TIDE and forwarding nominations from the feeder organizations, because they relied on nominating agencies to have done the all-source analysis. TSC officers rely mainly on the strength of the nominations as they receive them. (U//~~FOUO~~)

Closely related is the ambiguity surrounding TIDE. TIDE is the US Government's central repository of identities for known and suspected international terrorists; many in the Intelligence Community—and, based on press reporting, in Congress—believe that TIDE is the place where the intelligence and law enforcement communities can easily search for and piece together bits of terrorism-related information. In practice, however, TIDE is not that database. TIDE as it currently exists is largely a compilation of individuals who have been considered for watchlisting; individuals who fall below that threshold but who may nonetheless merit concern are not necessarily included. TIDE is not used as a dynamic tool that analysts populate with fragmentary intelligence to build, identify, and shape a dossier on a suspected terrorist. (U//~~FOUO~~)

With that in mind, we offer several recommendations.

- *The criteria and threshold for watchlisting need greater clarity.* Throughout our interviews we heard that different agencies use differing interpretations of the criteria for watchlisting nominations.[94] Regardless of where the threshold for derogatory information eventually settles, the Intelligence Community needs a single set of transparent guidelines that enables analysts to determine whether and when they may nominate a suspected terrorist. We agree with SSCI that TIDE administrators should accept nominations based on

partial names; terrorists rarely use full, true names in their clandestine communications.

- *We also caution against criteria that become too specific and caveat-laden.* If past experience is any guide, attempts to lend greater precision and add nuance only open the door to greater confusion when inherently subjective judgments are at play.[95] As SSCI recently observed, the standards to place an individual on a watchlist are simply too complicated.[96]

- *The Community needs to establish greater clarity on roles and responsibilities*, making clear that the nominating agency should see the nomination through from start to finish. NCTC plays a particularly important role tracking suspected terrorists who fall into the amorphous category that crosses between foreign and domestic jurisdictions.

- *We endorse the White House recommendation that NCTC develop a records enhancement capability that can build, locate, and track derogatory information on all individuals in TIDE—a process already underway.*

- *Watchlisting efforts should be streamlined and the resulting savings redirected.* Agencies such as CIA [redacted] have large staffs whose primary duties are data entry and processing before forwarding the nomination to the NCTC Watchlisting staff. Similarly, the primary duties of the NCTC Watchlisting staff are to enter and process the data before forwarding the nomination to TSC. Our interviews showed that such duplication has given each organization a sense that others were doing more than they actually did. Reducing some of this duplication could make available resources that could be redirected to other important watchlisting duties, such as records enhancement. IT improvements can simplify this process.

(b)(1)
(b)(3)
NSA

IT Could Do It: An Opportunity to Revolutionize the Community's Watchlisting Practices (U)

Our interlocutors often told us that the missed opportunities were not primarily an IT problem. Given the present state of IT in the relevant parts of the Intelligence Community—and the limited vision of what IT could be doing—this is true. But consider what would have been possible if modern IT were being used by the Community to assist with nominations for watchlisting:

- A system with the sophisticated entity resolution capabilities could automatically build and propose TIDE dossiers based on data available to NCTC.

- An algorithm could give these dossiers preliminary scores indicating the likelihood of meeting watchlist criteria, taking into account presence of the necessary identifiers (full name, date of birth, etc.) and signals of associated derogatory (i.e., membership in a terrorist organization).

- These computer-generated dossiers would flow to the watchlisting analysts for processing, with the relevant biographic and probable derogatory data highlighted. As new information came in, the computer would highlight it in the dossiers pushed to the analysts.

- While we cannot be sure without experimentation, we think it likely that over time the algorithms also could be trained to identify the probable watchlisting criteria that the dossier fits. ~~(S//NF)~~

- *Analysts need to use TIDE as a primary repository of intelligence rather than merely as a step in the watchlisting process.* In focusing on placing suspected terrorists on the No Fly list, the Community appears to have missed opportunities to use TIDE as a powerful tool for aggregating all derogatory and identity reporting on suspected terrorists; we recommend that NCTC take the lead in a Community-wide training program to help all agencies understand the purpose of TIDE, its holdings, and criteria for entry into TIDE. [redacted] which could have been matched [redacted] or which could have been fed into other watchlist databases. The fragmentary nature of counterterrorism reporting makes it imperative that analysts lean forward in populating TIDE with derogatory and partial identity intelligence rather than waiting to assemble a comprehensive intelligence package that meets all of the criteria for No Fly status.

(b)(1)
(b)(3)
NSA
CIA

- *The Community needs a standardized training program on the specifics of watchlisting.* We have seen some review groups claim that the 25 December incident proves a need for centralized analytic tradecraft training, but in our view a more pressing need—one clearly related to the Flight 253 incident—is a common and transparent understanding of the watchlisting process. If TSC remains the final voice in the No Fly/Selectee decision, it should be the lead agency to direct such a training effort, so that its standards are clear to all nominators. ~~(S//NF)~~

To summarize our recommendations, the Community should:

- ***Use all-source holdings for searches on terrorist identities; leverage technology such as "fuzzy logic" for name variants, and "discoverability" that advises when there is relevant information in another location; train officers to use all the salient details that can narrow the search and identify an individual.***
- ***Clarify the criteria for watchlisting in a way that does not become excessively specific, onerous, and legalistic.***
- ***Establish a training program that will provide greater clarity on the purpose of TIDE, the roles and responsibilities of agencies that may populate it, and how TIDE fits into the larger watchlisting process.***
- ***Instruct analysts to populate TIDE with partial derogatory information—making TIDE "the place to build a dossier"—rather than treating it as a library of completed watchlist nominations.*** ~~(C//NF)~~

Information Technology: Managing the Signals-to-Noise Volume

Inadequate information technology runs through both the Fort Hood and the NW Flight 253 narratives, particularly the inability of IT systems to help analysts locate relevant reporting in a sea of fragmentary data or to correct for seemingly minor human errors. The Intelligence Community's IT tools—which generally lag several years behind those of private industry, and even farther behind those available to home users—did not help intelligence officers and agents correlate data that could have increased the probability of Abdulmuttalab and Hasan rising above the noise. Indeed, the incidents highlighted what we assess are the two main technological problems facing counterterrorism officers:

- *Limited visibility and accessibility of counterterrorism data that are distributed across multiple, discrete databases and systems.* NCTC analysts, for example, have access to more than 28 separate databases and systems, each of which, for the most part, has a separate log-on. This means analysts have to search each database separately before trying to identify connections among their results.

- *Search capabilities do not allow full exploitation of existing data.* In most cases, users must know in advance what to look for using Boolean searches to find terms in individual reports as they are received by the Community. This approach is intolerant of even simple mistakes in the queries and does not enable questions like: list everyone that is potentially affiliated with AQAP and has a passport or visa that would permit entry to the United States or UK. ~~(S//NF)~~

In our view, these shortcomings are the result of a fundamental problem in the Community's approach to IT—there is no accepted and comprehensive, Community-wide strategy. The Intelligence Community lacks a common vision of a desired end state, a common understanding of the potential benefits, and a coherent Community-wide strategy for development and acquisition.

Better Results Come from Correlating More Data (U)

The Intelligence Community could have identified Abdulmutallab as the probable individual volunteering his services to AQAP in [redacted]—even if his father had never approached [redacted]

(b)(1) (b)(3) NSA CIA

- [redacted]

(b)(1) (b)(3) NSA CIA

- [redacted]

(b)(1) (b)(3) CIA

- [redacted]

~~(TS//SI//NF)~~

- Continuing the current course will become even more problematic as the amount of data increases and almost certainly ensures additional incidents in which the Intelligence Community discovers afterwards that it had access to data that would have enabled detection and potentially disruption of an attack.

- As the preparations for attacks are concealed more and more effectively, the planning periods decrease, and terrorists adopt new modes of attack improved information technology will be vital. The existing processes, policies, and operations will not suffice. ~~(S//NF)~~

We propose three sets of recommendations—near-, mid-, and long-term—that seek to enable faster adoption throughout the Community of IT solutions

that will reduce our reliance on human beings' inherently limited ability to sift and correlate vast amounts of data in their heads. Our recommendations range from incrementally upgrading existing applications to fundamentally reimagining the Intelligence Community's IT infrastructure; many can be accomplished in parallel.

- These recommendations are intended to serve only as a starting point. IT is a moving target, but waiting and debating in search of a comprehensive, perfect solution is dangerous; the important thing is to get started.

- When implementing these recommendations or taking any other steps to enhance the Community's IT infrastructure, it will be important to adhere to four key methodological principles: invest in computing capacity ahead of need, embed developers with users, adopt a modular approach based on separation of applications, data, and infrastructure, and experiment. Details of our proposed methodology for implementing these recommendations are found in Appendix C. ~~(S//NF)~~

We assess agencies' desire and need to protect some of their information will be the primary obstacle to implementing these recommendations, but this barrier is surmountable if policy, technology, and operations can co-evolve. Technologists need to demonstrate capabilities that instill confidence that access can be limited to authorized users, thereby addressing the concerns underpinning current information management policies. [redacted] shows that assessments of this tradeoff can change as new technologies are introduced.

(b)(1)
(b)(3)
CIA

- Many of the people we interviewed assessed that policy on handling US Persons data,[97] law enforcement data, and sensitive source data was limiting the Intelligence Community's ability to aggregate and exploit available data, especially information pertaining to critical domestic-foreign nexus issues.

- There is no perfect solution to the risk/benefit tradeoff on enabling correlation of data from the Community's most sensitive sources, but the counterintelligence calculus on terrorism data should be looked at through the prism of risk entailed in the event a terrorist act is not detected. ~~(S//NF)~~

Moving Forward on Information Technology. Our recommendations fall into three categories: near-term changes with limited resource implications, intermediate changes that require more time or resources, and longer-term efforts that we view as essential for the Intelligence Community to at least match capabilities already widely available outside the Community.

- Many of our recommendations are not novel. Several have been discussed for decades, and some already are underway.[98] We emphasize them here because we view them as essential for the Community to increase the likelihood that the right "signals" emerge from the "noise."

- For our recommendations to be effective, they need to be followed with particular urgency and fidelity by the four Intelligence Community entities with the broadest responsibilities for counterterrorism—CIA, FBI, NCTC, and NSA. There are no organizational barriers to these four agencies to collaborate to improve their ability to exploit data that they already share. (U//~~FOUO~~)

In the near term, the Intelligence Community must address the problem—as evidenced in both incidents—that many officers do not know what data they are accessing, what other relevant data exists, or how to exploit it.

- Greatly increase online documentation related to datasets by, for example, tagging and registering them. This information should be easily accessible and include what data are available, how to get access, who has access, and tips from experienced users.

- Enable authorized users to access and use all-source data and applications from anywhere and at anytime, except when reasonably prohibited by security concerns. The 25 December incident

highlighted that officers in the field sometimes are best positioned to separate signal from noise.

- Search capabilities should default to the use of fuzzy logic. Had this been the case in November, the State Department's Visas Viper cable, despite the misspelling, would have prompted discovery of Abdulmutallab's active US visa.

- Embed IT specialists in fast-moving analytic and operational groups to handle simple support requests immediately. The Community should not continue to allow mundane IT problems to interfere with its mission.

(b)(1) (b)(3) CIA

- [redacted] ~~(TS//SI//NF)~~

In the midterm, but sooner rather than later, the Intelligence Community must enable persistent search, exploit query logs, attach analytic insights to data, facilitate continuous IT improvements, and bridge the data divide—while building toward the long-term vision. To do this, the Community must:

- Augment current search capabilities with user-controlled alerting services that would flag incoming traffic and automatically correlate it with existing reporting. [redacted]

(b)(1) (b)(3) (b)(7)(E) FBI

- Enable officers across the Community to see who else has looked at a given intelligence report and to electronically attach informal insights and view comments by others. This may have enabled broader discussion among analysts interested in a Nigerian affiliated with AQAP or in Hasan and Aulaqi.

- Embed developers with users to provide continuous improvements to mission applications. This would foster innovation by giving developers—who can imagine what technology can deliver—a better understanding of end-users' requirements.

- Incorporate application programming interfaces (APIs) into all existing programs so that they can be accessed, as appropriate, through other programs. This would, policy permitting, enable officers to access multiple databases, across multiple networks, through a single software interface.

- Incorporate into new and existing programs the capability to load large amounts of data for bulk searches. [redacted] ~~(TS//SI//NF)~~

(b)(1) (b)(3) ODNI

In the long term, we make three recommendations to help ensure the Intelligence Community provides its counterterrorism officers with state-of-the-art capabilities for search and correlation. Several technical leaders in the Community are working on ideas similar to or consistent with these; we offer our perspective to encourage and help shape these efforts. (U)

First, enable a federated and cross-domain search. This would be a minimal step toward modernizing the Community's search capabilities and ameliorating some of the problems posed by the proliferation of databases across networks. Developers would place a thin layer over existing databases that would provide a single point of entry to query—through an API—each database to which they are authorized access. This would minimize the extent to which officers must remember where to search for what data and simplify officers' synthesis of the results. (U)

Second, separate applications from data and infrastructure. This would enable authorized

---

[1] The FBI has already implemented a new tool in DWS— [redacted] ~~(S//NF)~~

(b)(1) (b)(3) (b)(7)(E) FBI

intelligence officers to access and use any data, anytime, from any workplace, with any tool, except as policy prohibits it. The most important initial step is to establish the virtual equivalent of the now-common Community badge: a common way of identifying individuals and their access permissions together with tagging of the data to describe the rights needed to access it.

- We endorse the joint effort of various agencies, working through their chief information officers, to build toward a common IT infrastructure and identify common data services, such as those for collaboration, access, discovery, audit, processing, and storage.

- A common infrastructure for all data would have many advantages, including enabling the use of sophisticated search algorithms such as those used on the Internet, instead of the outdated Boolean searches currently used on most Intelligence Community systems. Another benefit would be the capability to allow a user to file all relevant data on one interface, rather than on a system-by-system basis. (U//~~FOUO~~)

Third, build computing clouds and data centers—which will enable dispersed, enterprise data sharing and processing—as the basis for the Community's IT infrastructure. The resultant computing capacity will allow "data to talk to data," identify relationships, produce results that analysts now have to put together by hand, and do it before an officer has even thought to make an inquiry. Routine use of this kind of processing almost certainly would have helped identify Abdulmutallab for watchlisting.

- Additional advantages of a cloud-based approach include lower overall costs, greater flexibility in the use of resources, ease of maintenance, and easier portability of innovations. Private-sector technology leaders such as Microsoft, Amazon, and Google build their systems using clouds.

- As the Intelligence Community moves toward the cloud, it will need to adopt—at the Community level—hardware, operating systems, and networks. All new systems should be expected to use this common base. ~~(S//NF)~~

We also endorse two current initiatives that are necessary precursors for the Intelligence Community to move toward cloud computing:

- We believe investment in the I2 Cloud Pilot, which will facilitate enterprise data processing and storage, is critical to modernizing the Community's use of information technologies.

- [redacted] ~~(S//NF)~~ (b)(1) (b)(3) CIA

Our recommendations in this area are much more complex than elsewhere and resist simplification. Nonetheless, to summarize:

- ***In the near term, take the steps detailed above to ensure that counterterrorism officers understand all of the data available to them and have the tools to access what already exists—when they need it and where they need it.***

- ***In the midterm, augment capabilities to get more out of the data with tools that allow officers to learn more from the data than what it presents on the surface—who has seen it, what others think of it or have done with it, what related data is available, and how it relates to historical reporting.***

- ***In the long term, move beyond an architecture that relies so heavily on human initiative to one in which "data can talk to data"—so that relationships embedded in complex datasets are brought to the surface in ways that move the analyst's starting point further down the field and closer to discovery of an adversary's plans and intentions.***

- ***Pursue these objectives on a "crash" basis. The panel is convinced that delay will assure that more Umar Farouks get through. (U//~~FOUO~~)***

Is Information Sharing a Problem? (U)

Various review groups and agency-specific memos have concluded that information sharing was not a significant factor contributing to the incidents at Fort Hood and on 25 December; we agree with that broad conclusion. Some issues that surfaced, while not directly tied to the Fort Hood or 25 December incident, merit follow-up to determine whether these issues impede the counterterrorism mission:

- FAA officers said that analysts there have uneven access to FBI threat reporting and no access to TIDE because FAA is not part of the Intelligence Community.[99]

- TSA officials noted that a lack of information sharing with counterparts abroad may limit cooperation if TSA cannot share threat reporting to make its case for implementing specific—and often costly—countermeasures. ~~(C//NF)~~

Going forward, the Community must make breakthroughs on information sharing policy and its implementation to reap the benefits of information technology. Policy must be tailored to enable authorized users to access and use all-source data and applications from anywhere and at anytime—except when reasonably prohibited by security concerns.

- Intelligence Community Directive 501, Discovery and Dissemination or Retrieval of Information within the Intelligence Community, codifies procedures for discovery and sharing of data. These procedures enable authorized Community users to "discover" relevant data in other agencies' holdings and—if they do not already have access—find a point of contact to request access. Thus, it effectively lays the policy groundwork for implementing our recommendations on information technology.

- The Community should develop an integrated approach to information sharing with US government entities outside the Intelligence Community, i.e., "non-Title 50 organizations." Efforts already are underway, but an integrated approach would help clarify what information the Community can access from non-Title 50 organizations, and what those organizations need in return from the Community.

- *Procedures for sharing information on US Persons must be clarified and better explained.* We detail these at length in a separate section. The Community cannot realize the potential of information technology to assist the counterterrorism mission without clarifying these issues. (U/~~/FOUO~~)

On a cautionary note, some of the proposed remedies on information sharing strike us as unwise or overly broad. For example, SSCI recommends expanding access to [redacted] There are other ways to increase counterterrorism officers' ability to discover foreign intelligence information without jeopardizing [redacted] and access while mitigating risk to sensitive operational data. ~~(S//NF)~~ (b)(1) (b)(3) CIA

Closing the Structural Seams in the Intelligence Community's Counterterrorism Mission
We observed a third set of problems related to the roles and responsibilities of the Community's counterterrorism efforts. We began this review with the view that the redundancies in the Community's counterterrorism efforts represent healthy competition and that "lanes in the road" issues in no way directly contributed to the Fort Hood or 25 December incidents. Officers we interviewed consistently said that turf considerations and bureaucratic overlap did not play a direct role either incident. (U~~//FOUO)~~

There is no way for the panel to produce a definitive assessment on that point, but there are grounds for skepticism. The panel is concerned that the overlap between CTC and NCTC extends beyond healthy competition and that the turf battles, duplications, and clashes are a drain on the resources and creative energy of both organizations. This is concerning in part because both organizations stressed to the panel that they did not have enough resources to cover all issues at the level they deserve. Moreover, given the labor intensive nature of counterterrorism work, any wasted energy only exacerbates the "signals to noise" problem—which could hamper the Community's ability to detect and prevent the next Abdulmutallab-like attack. The panel believes, therefore, that there is still work to be done in sorting out the mission of these two important organizations. (U~~//FOUO)~~

Create a formal division of labor that plays to the clear strengths of each organization. From the moment NCTC was codified in the 2004 Intelligence Reform and Terrorism Prevention Act (IRTPA)—transforming the threat orientation of its predecessor, the Terrorist Threat Integration Center, into the primary responsibility for the analysis of terrorism—it was inevitable that there would be problems of deconfliction between it and CIA's CTC, given that the analytic portions of the two organizations have so much overlap in their missions and draw to a large extent on the same limited talent pool. The panel discussed the implications of merging the analytic function of these two entities but concluded each has distinct, essential missions that require emphasis—detecting and identifying threats to the homeland and supporting counterterrorism operations abroad. (U~~//FOUO)~~

Over the years, much effort has gone into formally codifying the "lanes in the road" for each to follow, and we cannot improve on the DNI directive of 7 April 2010 (see Appendix D), which embodies many of the views we expressed in the course of our discussions with NCTC, CIA, and the DNI. Clarifying these roles and responsibilities will, we think, improve mission performance, reduce bureaucratic conflict, and avoid reforms that could be counterproductive. In the end, it must fall to leadership and management to marshal the talents of their people and the mandates of their organizations in ways that are mutually reinforcing and that close whatever gaps open up in our counterterrorism coverage.

- NCTC's relationships with FBI and DHS, legislative authorities, and tie-in to the homeland make it the natural lead for tracking and warning of all foreign threats with the potential to reach US soil.

- CTC, on the other hand, is the natural lead on terrorist operations abroad, particularly involving support for operators and collectors. ~~(S//NF)~~

It appears that much of the tension between the two organizations centers on issues related to the President's Daily Brief (PDB)—everything from who takes the lead to what is said in the articles. The panel believes it is not necessary to implement the change proposed in the ODNI's "Counterterrorism Review Master Action Plan: 6 Month Priorities." This recommends that "NCTC leads PDB planning process" on counterterrorism-related stories. The PDB is already a Community-wide publication, and ODNI officers on the PDB leadership team already have the authority to task agencies to track and write about specific issues. We think that exercising current authorities could achieve the same goal—integrated analytic coverage—with considerably less disruption and bureaucratic layering. ~~(S//NF)~~

We are skeptical of any division of labor that divides counterterrorism responsibilities

exclusively along "tactical" and "strategic" lines. Terrorist organizations do not function that way, nor do analysis and collection. It is impossible to perform tactical analysis without an understanding of strategic goals, and it is impossible to understand an organization's strategy without a grasp of how and why it conducts specific operations. ~~(S//NF)~~

Dramatically increase the focus on threats to the homeland. As we observed the segmented nature of following terrorists bound for the homeland—and the associated problem with bureaucratic handoff as the threat moves from the foreign to domestic realm—we became firmly convinced of the need for a unit that would lead the Community in tracking all threat reporting that hinted at an attack against the homeland. While all agencies should focus on threats to the homeland as their greatest priority, one organization needs to have sole responsibility for tracking, warning, and coordinating the Community's response to all threats with the potential to reach US soil. We think NCTC is a natural fit for this role. (U/~~FOUO~~)

For this reason, we strongly endorse NCTC's concept of a "pursuit group." The goal of this group, as we understand it based on the DNI's recent memo,[101] would be to provide analytic and analysis-driven insight and tasking for follow-on collection to establish the underlying basis and provide additional information useful to thwarting the plot. As that group develops its concept of operations, we offer five recommendations:

- It must emphasize primarily threats with the potential to reach the homeland, avoiding the natural temptation to fall back into the traditional, more familiar terrain of focusing mainly on threats overseas;

- The organization must place a particularly heavy emphasis on areas where we have limited or emerging coverage;

- It must deconflict and coordinate its pursuit of targets with other Community components so that multiple units are not duplicating the efforts of another;

- It should develop a coherent set of indicators that will help identify when terrorist groups abroad are adopting a focus on the US homeland; [redacted] (b)(1) (b)(3) ODNI

- Its metric of success should be tapping the full range of US government capabilities to identify and disrupt plots—not traditional metrics such as production of finished intelligence. ~~(C//NF)~~

Increase "jointness" within the counterterrorism community. No mission in the Intelligence Community is more important than preventing terrorist attacks inside the United States; it requires seamless collaboration, from collectors in the field to consular sections, airport screeners, law enforcement and intelligence officers, and policymakers. (U)

Yet the process is still too fragmented and segregated. In our review of the Abdulmutallab and Hasan cases, we noted that contacts and information flow between agencies were often uncertain, frequently based on personal connections and individual initiative rather than institutional arrangements. To cite only a few examples, CTC, NCTC and NSA officers often commented on the central role of TSC. Watchlisting officers explained that the normal process required time to move a nomination through to a TSC decision, but when the situation required rapid action, telephone calls to personal contacts at TSC could expedite the process, taking hours rather than days. Embeddedness of NSA and CIA officers at TSC, and vice versa, has been uneven. Similarly, embedding more TSA officers in those agencies could facilitate the process of delivering downgraded tearlines pertaining to aviation threats.

- Increase the number and frequency of personnel rotations between CTC and NCTC—not just among line analysts, but among senior managers, as well. These should be mandatory and take place with regular periodicity. We suspect these moves would foster collaboration as each side views the lanes in the road issue while driving on the opposite side of the road.

- We agree with the West-Clark review of the Fort Hood incident, which noted the need for greater collaboration between FBI and DoD; there also were no counterintelligence officers from the Department of the Army, CIA's Counterintelligence Center, or the DNI's National Counterintelligence Center supporting either the Washington or the San Diego JTTF.[102]

- "Jointness" can also be pursued as a performance objective at the individual level. As a small step toward developing a culture of collaboration, an explicit performance objective for all CTC and NCTC analysts should be to conduct one joint project per reporting cycle with their primary counterparts from the other organization. Officers should be evaluated specifically on whether they meet that objective. ~~(C//NF)~~

To summarize our recommendations:

- ***Organizational responsibilities should play to the comparative advantage of each organization. In practice, this means that NCTC's relationships with FBI and DHS, its legislative authorities, and its tie-in to the homeland make it the natural lead on all threats with the potential to reach US soil. CTC, on the other hand, is the natural lead on terrorist operations abroad, particularly involving support for operators and collectors. Focusing on this approach would, we suspect, reduce the time-consuming turf disputes over PDB authorship.***

- ***Wherever Intelligence Community leaders draw the "lanes in the road," some component must focus tirelessly and exclusively on following all reporting that involves threats to the US homeland. This needs to be a primary focus of NCTC's new pursuit group, as it develops fragmentary data that raise concerns about terrorism but lack specificity.***

- ***To improve seamlessness throughout the intelligence and law enforcement communities, agencies should increase the rotation of officers among these organizations.*** ~~(C//NF)~~

Clearing the Way for Properly Sharing US Person Information

Throughout our interviews, we were impressed with the great care taken by the Community to protect information about US Persons.[m] [103] We noted, however, that US Persons issues manifested themselves in several ways in these cases.

- Sharing US Person information with foreign partners, and tasking them to collect on US Persons appeared at various points. [redacted] (b)(1) (b)(3) NSA

- [redacted] (b)(1) (b)(3) NSA

- Intelligence officers in both the 25 December and the Hasan cases worked hard to stay within authorized guidelines, which sometimes led to excessive caution. [redacted] (b)(1) (b)(3) ODNI

(b)(1) (b)(3) (b)(7)(E) FBI

[m] A US Person is defined by Executive Order as including not only an American Citizen and Lawful Permanent Resident, but also a corporation incorporated in the United States, and an unincorporated association substantially composed of citizens and lawful permanent residents. (U)

(b)(1)
(b)(3)
(b)(7)(E)
FBI

[redacted]

- [redacted]

(b)(1)
(b)(3)
(b)(7)(E)
FBI

(b)(1)
(b)(3)
NSA
CIA

~~(TS//SI//NF/~~ [redacted]

In general, we noticed a strong belief among collectors and analysts that restrictions on collecting, disseminating, accessing, and analyzing data on US Persons impede mission performance. A high-level NCTC official listed enhanced authorities related to US Persons as the number-one item on his wishlist of proposed reforms. [redacted] Information sharing often slowed considerably when it ran against actual or perceived issues relating to US Persons information. ~~(C//NF)~~

(b)(1)
(b)(3)
NSA

We also saw a surprising level of disagreement—even among experienced practitioners—on whether current US Person authorities allow intelligence officers to accomplish their missions, or whether new legal authorities are needed.

(b)(1)
(b)(3)
NSA

- For example, we heard strong views on whether [redacted]

[redacted]

(b)(1)
(b)(3)
NSA

- Similarly, NSA officers noted that if they were surveiling a suspected terrorist overseas whom they thought to be a non-US Person, and they later learned that he was a US Person, they had to cease collection while they sought separate court authorization to re-initiate collection, resulting in another collection gap.

- [redacted] ~~(S//NF)~~

(b)(1)
(b)(3)
NSA

Panel members with deep experience on FISA and related matters provided a different perspective. They believe that current authorities, when clarified and fully leveraged, should enable the government to accomplish its counterterrorism mission.

- For example, they believe that the Community's current authorities enabled the government to adequately surveil US Persons globally and suspected terrorists inside the United States—and to share lawfully collected telephone numbers in shared databases—while also protecting privacy and civil liberties.

- The experience of these panel members leads us to believe that the government must develop more efficient processes to make effective use of existing authorities, especially ones that focus on

(b)(1)
(b)(3)
NSA

recurring situations. [redacted]

- In general, the law and the Community's governing Executive Order (EO 12333) provide the government with the operating room to be effective; most of the burdensome steps appear to be internal to the government's implementing procedures—which could cause the collection gaps and other issues described to us.

- Fixing these procedures is not solely the responsibility of any single agency or of the DNI. This requires the Department of Justice continuously to engage with the DNI, both to calibrate on an ongoing basis how to craft the procedures so that they clearly and straightforwardly implement the Community's governing legal requirements, and to provide assurance that when the Community complies with those procedures, it is following the law. ~~(S//NF)~~

We believe that the Community's culture of carefully protecting US Person information is vital for earning and maintaining the trust of the American people and of oversight bodies. The Community must have that trust so that it can make the most of existing authorities—and obtain new ones as needed—to counter a rapidly evolving terrorist threat.

- Indeed, we believe that in that light, it is all the more important to streamline and clarify policies and procedures—to ensure they are being used to protect privacy and civil liberties interests and implement legal requirements, rather than to serve other purposes.

- To be an effective part of the intelligence mission—and not be an "impediment"—policies and procedures must be focused, clear, easy-to-understand, and consistent across agencies where feasible. We believe much work lies ahead to achieve that. ~~(S//NF)~~

Collectively, these US Persons issues can and must be addressed in the near term. Some involve closing the breach between the perceptions and realities of current US authorities; others entail changing internal procedures of individual agencies. All involve focused leadership from the DNI, in concert with the Department of Justice. We understand that this important work has already begun (see Appendix B). (U)

We see a need to simplify, harmonize, update, and modify the Community's procedures relating to US Persons. We also see a clear need for standardized, continual Community-wide training and guidance on how to address US Person issues.

- The goal of such efforts is twofold: First, to make use of the Intelligence Community's authorities to the full extent intended, so that the Community can more efficiently manage the information in its possession and correlate data as envisioned by the IT recommendations. Second, to help intelligence officers better understand what they need to do to collect and share information with confidence that their actions are consistent with legal and privacy requirements.

- It is especially important that these efforts focus on working-level analysts and collectors who are most directly affected by US Persons considerations, to dispel any misperceptions, and to elicit areas where training, guidance, and updated procedures could facilitate intelligence operations while still protecting privacy and civil liberties interests. For example, working-level officers should be provided a consistent, clear, authoritative—and preferably online—guide, with the assurance that following it provides a "safe harbor" on US Persons issues. (U)

We also recommend that the DNI establish a Community-wide, inter-disciplinary process for determining whether new authorities may be needed, on emerging issues, such as radicalization, new technological developments, and new forms of terrorist communication. The goal would be to provide clarity and confidence to operators and analysts so that they know how conduct their missions in a way that properly protects privacy

and legal interests, clearing the way for decisive action.

- If, as we suspect, terrorist means of communication increase in sophistication and self-radicalization inside the United States becomes a more pressing concern, it will be increasingly urgent to regularly bring together analysts, collectors, and attorneys to discuss whether current authorities and guidance are keeping pace with the evolving nature of the terrorist threat.

- Regarding working with liaison partners, we recommend all agencies actively engage key liaison partners to develop plans to ensure collection in a way that is consistent with any protections for US Persons. The Community will benefit from a review of procedures for sharing with liaison services when it has authority to collect on US Persons and is seeking liaison assistance in such cooperation.

- Our recommendation in this area is an expansion of SSCI's sensible guidance that NSA should conduct such an effort with its foreign partners. ~~(S//NF)~~

To summarize:

- ***Protecting US Person information is vital for accomplishing the intelligence mission; the rules for doing so must be focused, clear, easy-to-understand, and consistent across agencies where feasible.***
- ***The DNI must, in concert with DOJ, lead a Community-wide effort to provide training and guidance on US Person policies and procedures, and to simplify, streamline, update, and harmonize them where feasible, with the goal of providing Community operators and analysts the confidence they need to do their jobs knowing that they are properly protecting privacy and complying with the law.***
- ***The Community should engage with liaison services to clarify and streamline its procedures for properly collecting and sharing US Person information.***
- ***The DNI should establish an inter-disciplinary process for providing guidance and clarity on emerging issues relating to US Persons, such as radicalization, new technologies, and new forms of communication.*** ~~(S//NF)~~

Abdulmutallab, Hasan, and Radicalization (U)

Despite the many differences between the two incidents,[104] a common thread through both of them was what the Intelligence Community has termed "self-radicalization." During our review, we came away with four recommendations related to this issue. (U/~~FOUO~~)

First, the Community should accelerate its efforts to understand homegrown radicalization. This is among the areas from which intelligence surprise could spring in the absence of a template to inform the Community's collection and analysis, a point made by outside experts. While the Community has longstanding initiatives to study radicalization overseas, its efforts to understand homegrown radicalization are more nascent. Developing a grasp of the issue may require new types of expertise and collection across the Community, as the United States provides a unique and diverse environment for radicalization. It will also require a robust understanding of, and respect for, civil rights and liberties. ~~(C//NF)~~

Second, we agree with the experts we consulted who recommended that the Community sharpen its focus on recruiters and enablers, how disaffected individuals radicalize (through groups, in prisons, on the Internet), and how they influence an individual's efforts to become operational. As some analysts pointed out to us, "self"-radicalization may be a misnomer. Hasan and Abdulmutallab were influenced by radicals—Aulaqi in both cases, but to differing extents—and by the Internet, which will play an increasing role in radicalization in the future.

- The Community also must develop methods for detecting radicalized individuals or "lone wolves" who may not have attended terrorist training camps or may be operating outside the direct command and control of organized groups. The Community currently faces a signals-to-noise challenge with such individuals overseas, and must find ways to identify such individuals inside the United States while respecting civil rights and liberties—and retaining and enlisting the support of local communities. ~~(C//NF)~~

Third, the lessons learned from studying the radicalization and self-radicalization of US Persons—such as Hasan—should be incorporated as appropriate into counterintelligence and US Government personnel policies, which are typically designed to detect traditional state-versus-state spying.

- When government employees are involved, bringing counterintelligence professionals into the investigative process early can significantly increase the probability of detecting at-risk individuals.[n]

- As in other counterintelligence cases (Ames, Hanssen), the Hasan episode underscores the importance of documenting and maintaining in an individual's permanent record all relevant information about his or her performance.[105] ~~(C//NF)~~

Finally, we believe it is vital to properly align organizational responsibilities related to radicalization with each agency's strengths and authorities. NCTC, FBI, and DHS must play their respective parts in close collaboration with one another. FBI's unique strengths include robust legal authorities and direct experience investigating domestic and international terrorism inside the United States; those of NCTC include analyzing radicalization, bridging the foreign/domestic divide, and accessing intelligence from across the Community. DHS is uniquely positioned to focus on analysis relevant to infrastructure vulnerabilities and domestic protective measures; aggregating data uniquely available to DHS for use by the counterterrorism community; and working with state, local, tribal, and private-sector customers. We recommend that the Community reassess its assignment of radicalization-related responsibilities among these key organizations to ensure that they are bringing to bear their unique strengths and authorities on this critical issue. ~~(S//NF)~~

(b)(1)
(b)(3)
(b)(7)(E)
FBI

[n] [redacted] ~~(S//OC/NF/~~[redacted]

(b)(1)
(b)(3)
NSA

Blue Sky Ideas (U)

The foregoing recommendations cover much of what the panel was asked to address. We have focused on recommendations that, while difficult, are still achievable within an individual agency or with DNI lead authority. Consistent with the third task assigned to the Review Panel, we offer several additional "blue sky" recommendations—ideas that we have not seen surfaced by other review groups and that would entail more radical changes. These ideas are deliberately provocative, and more disruptive to personnel resources and organizational structures, requiring more study before attempting.

- ***A Manhattan Project for information technology and sharing***. To break the gridlock and the ever-elusive search for the perfect IT architecture, we propose the chief information officers from the key intelligence agencies—along with their budgets—be pulled together into one unit with the goal of implementing a common infrastucture across the Intelligence Community. The Community has been wrestling with data-sharing adjustments for years with scant progress.

- ***Revisit the matrix option.*** The "matrix model" of organization [redacted]s one way to leverage the strengths of CTC and NCTC while reducing redundancy. A matrixed group can consist of analysts from CIA, NCTC, DIA, FBI, and NSA, who sit side-by-side with collectors and operators from the NCS, DoD, and NGA, all working under a common management structure that reports to both CTC and NCTC. [redacted] This model works best targeting specific issues involving a blurry line between domestic and foreign components and where there are relatively few analysts in relation to the workload. Using the matrix model also reduces redundancies related to dual publications, representation at interagency meetings, and responses to taskings.

(b)(1)
(b)(3)
CIA

- ***Leverage the expertise of INR and DHS/I&A.*** In our discussions of the Intelligence Community's counterterrorism efforts, we heard only few references to the State Department's Bureau of Intelligence and Research and DHS's Office of Intelligence and Analysis as key players. An institutional division of labor, in which INR and DHS/I&A have lead responsibility on some region or aspect of terrorism, could tap their expertise and increase efficiency in the Intelligence Community. DHS/I&A, for example, is uniquely positioned to assess US vulnerabilities—infrastructure, telecommunications and energy grids, and information-sharing gaps between national and local law enforcement.

- ***Expand the Intelligence Community's role in the visa issuance process.*** DHS could play an especially important role in the visa issuance process. Preventing terrorists from entering the US homeland is a top national security concern, so it makes little sense to place the visa issuance process in the hands only of foreign service officers. This responsibility should belong in the homeland security apparatus. If the suggestion is too burdensome for DHS, then consideration ought to be given to ensuring that all visa issuances require Community concurrence or are passed through the Community for examination.

- ***Build a counterterrorism-specific "Name Trace Central."*** Identity information is currently pocketed across the Intelligence Community in various databases, meaning no one officer in any agency can successfully access it. To remedy this, create a single unit, staffed by counterterrorism specialists from throughout the Community cleared for access to all relevant sources, responsible for counterterrorism-related name traces. Names traces would be conducted against holdings of all intelligence and law enforcement databases. ~~(S//NF)~~

Expert Perspectives: The View from "Insiders" and "Outsiders" (U)

We convened two expert roundtable sessions, one internal and one external, to stimulate our thinking about the Intelligence Community's posture to address issues beyond those surfaced during our review. The internal group of experts focused on threats that could surprise the Community and threats of which it is cognizant but not prepared to address. Among their key concerns were:

- [redacted]

(b)(1)
(b)(3)
CIA

[redacted] ~~(S//NF)~~

We asked the external group to address how the terrorist threat to the United States is changing; what terrorists could do to surprise the Intelligence Community or elude US countermeasures; what more the United States could do to protect itself; and to identify aspects of the terrorist problem that the United States is not focusing on, but should. (U//~~FOUO~~)

Those experts emphasized the following issues:

- The terrorist threat is heterogeneous—there is no longer a single "they," if there ever was;
- There are inherent difficulties in obtaining the key, plot-specific information that would allow the Intelligence Community to pull a thread that would uncover a plot. As a result, the Community will not always succeed—a terrorist will eventually get through US defenses;
- Tradeoffs must be made—within and outside the Community—that have real consequences, such as those between civil liberties and increasing the number of people on watchlists;
- Almost every foreign threat to the homeland that the United States has thwarted was uncovered because of foreign travel or communication; we are too dependent on these and need to develop and refine new detection strategies;
- The Intelligence Community should focus more on the key people and networks that enable disaffected individuals such as Hasan or Abdulmutallab to become operational, i.e., Aulaqi-like figures that inspire, enable, or recruit;
- The Community requires a well-developed model of the radicalization process from which it can derive indicators of an individual's propensity to adopt violent tactics. We have a strategic template for understanding foreign-based threats. We do not have one for the homeland. (U//~~FOUO~~)

To summarize, these two groups added to the panel's thinking by driving home several key points. Among them:

- ***The increasing urgency of homeland-related threats—and the need for a more sustained, cross-agency focus on this set of issues.***

- ***The increasing heterogeneity of the terrorist phenomenon, and therefore the growing challenge of detection and disruption.***

- ***The fragility of many of the collection techniques that help account for the Community's success so far.***

- ***The likelihood that terrorists will continue to behave in "learning" mode—adjusting their methods of operation, whether successful or not, in response to what they see us doing.*** ~~(S//NF)~~

Some Closing Thoughts (U)

While we have limited our review to the Intelligence Community, we come away convinced that strengthening the United States' ability to prevent the next Fort Hood or 25 December-like attempt requires focusing on more than just the Intelligence Community: law enforcement, airport security, the policy community, foreign partners, and even the private sector need to address the systemic issues that made the Fort Hood and 25 December incidents possible. At the risk of falling back on a cliché, we are reminded of the axiom that a chain is only as strong as its weakest link. Improved collection will not matter without sound analysis. Sound analysis will not matter without a robust watchlisting system. A robust watchlisting system will not matter without effective airport screening technology. Better screening technology will not matter without skilled screeners. There are multiple variations one could make on this chain of events, such as the vital role of foreign screeners at airports abroad—but all would reinforce the same point: the Intelligence Community is only one of several layers of homeland defense. (U)

To finally defeat terrorism requires at least three things: destroying the leadership, denying it safehaven, and changing the myriad conditions that give rise to the phenomenon. *The Intelligence Community can carry much of the burden on the first two—but very little on the third.* (U)

Constancy of support for the Intelligence Community is crucial. Intelligence stands apart from politics, but policy toward intelligence is formulated in a political environment. We cannot emphasize enough that the pendulum swings and ebbing and flowing of support is an obstacle to mission performance. NCTC, for example, was slated to lose roughly 35 positions prior to 25 December. The post-Christmas reaction to Flight 253 has caused watchlisting nominations to skyrocket; warning has become so common that the Community risks creating its own signals-to-noise problem. We have seen the same pendulum swings on the collection side, where agencies—acutely aware of controversies since 9/11—have erred on the side of caution, sometimes unnecessarily, slowing the dissemination of valuable intelligence. The Community's Congressional overseers have a vital role to play in helping to stabilize counterterrorism policies and keep them on a steady course. (U)

Appendix A

Consolidated List of Intelligence Community Review Panel Recommendations (U)

Build Internal Processes that Help Find Terrorists in the Data (U)

All agencies should…

- Disseminate counterterrorism reporting promptly.
- Update, standardize, and simplify their dissemination lists and codes on a regular basis.
- Search for terrorist identities against all of their available data holdings.
- Use technology such as "fuzzy logic" for name variants and incorporate "discoverability" that advises when there is relevant information in another location.
- Train officers performing identity searches to look for partial names, along with salient points such as the person's location, affiliations, passport numbers, schooling, or travel—details that can further narrow the search and identify an individual. ~~(S//NF)~~

The DNI should…

- Clarify the criteria and threshold for watchlisting. The Community needs a single set of transparent guidelines that enables analysts to determine whether and when they may nominate a suspected terrorist. We caution against criteria that become too specific and caveat-laden.
- Establish greater clarity on watchlisting roles and responsibilities. Delineate roles that play to each agency's particular strengths and authorities, and make clear that the nominating agency should see a nomination through from start to finish.
- Streamline watchlisting efforts and redirect the resulting savings. Reduce the duplication resulting from multiple agencies processing nominations and redirect the resources toward other pressing duties such as records enhancement. IT improvements can help simplify this process.
- Ensure analysts use TIDE as a primary repository of intelligence rather than as a step in the watchlisting process. The Community appears to be missing an opportunity to populate TIDE with fragmentary intelligence to build, identify, and shape dossiers on suspected terrorists. NCTC should lead a Community-

wide training program to help agencies understand the purpose of TIDE, its holdings, and criteria for entry into TIDE.

- Institute a Community-wide training program to ensure a common and transparent understanding of the watchlisting process. If TSC remains the final voice in the No Fly/Selectee decision, it should lead such a training effort, so that its standards are clear to all nominators. ~~(S//NF)~~

We also endorse…

- SSCI's recommendation that TIDE administrators accept nominations based on partial names. Terrorists rarely use full, true names in their clandestine communications.

- The White House's recommendation that NCTC develop a records-enhancement capability to build, locate, and track derogatory information on all individuals in TIDE. ~~(S//NF)~~

Develop Information Technology That Helps Separate Signals from Noise (U)

In the near term, all agencies should…

- Greatly increase online documentation related to datasets to show what data are available, how to get access, who has access, and to provide tips from experienced users.

- Enable authorized users to access and use all-source data and applications from any workplace and at any time, except when reasonably prohibited by security concerns. The 25 December incident highlighted that officers in the field sometimes are best positioned to separate signal from noise.

- Ensure that search capabilities default to the use of fuzzy logic. This would include the automatic incorporation of variant spellings and renderings of foreign names.

- Embed IT specialists in fast-moving analytic and operational groups to handle simple support requests immediately. The Community should not continue to allow mundane IT problems to interfere with its mission. ~~(C//NF)~~

In the midterm, all agencies should…

- Augment current search capabilities with user-controlled alerting services that flag incoming traffic and automatically correlate it with existing reporting.

- Enable officers to see who else has looked at a given intelligence report and to electronically attach informal insights and view comments by others. Such a capability may have enabled broader discussion among officers interested in a Nigerian affiliated with AQAP or in Hasan and Aulaqi.

- Embed developers with users to provide continual improvements to mission applications and give developers a better understanding of end-users' requirements.

- Incorporate application programming interfaces (APIs) into all existing programs so that they can be accessed, as appropriate, through other programs. This would, policy permitting, enable officers to access multiple databases, across multiple networks, through a single software interface.

- Incorporate into new and existing programs the capability to load large amounts of data for bulk searches, giving analysts the capability compare discrete datasets in [redacted] ~~(S//NF)~~ (b)(1) (b)(3) ODNI

In the long term, the DNI should…

- Enable a federated and cross-domain search across all of the Community's holdings. Developers would place a thin layer over existing databases that would provide users a single point of entry to query each database they are authorized to access.

- Establish the virtual equivalent of the Community identification badge: a common way of identifying individuals and their access permissions together with tagging of the data to describe the rights needed to access it. This is a key step toward building a shared network and common approach to sharing data and toward enabling authorized intelligence officers to access and use any data, anytime, from any workplace, with any tool, except as prohibited by policy.

- Build computing clouds and data centers as the basis for the Intelligence Community's information technology infrastructure. As the Community moves toward the cloud, it will need to adopt—at the Community level—hardware, operating systems, and networks. All new systems should be expected to use this common base.

- Adhere to four key methodological principles—invest in computing capacity ahead of need; embed developers with users; adopt a modular approach based on separation of applications, data, and infrastructure; and experiment—when implementing any changes to the Community's information technology. (See Appendix C.) ~~(S//NF)~~

We endorse…

- The I2 Cloud Pilot, which will facilitate enterprise data processing and storage and is critical to modernizing the Community's use of information technologies.

- [redacted] (b)(1) (b)(3) CIA

- The joint effort of various agencies, working through their chief information officers, to build toward a common IT infrastructure and identify common data services, such as those for collaboration, access, discovery, audit, processing, and storage.

- [redacted] ~~(TS//SI//NF)~~ (b)(1) (b)(3) CIA

Close the Structural Seams in the Counterterrorism Mission (U)

The DNI should…

- Dramatically increase the focus on threats to the homeland. While all agencies should focus on threats to the homeland as their greatest priority, one organization needs to have sole responsibility for tracking, warning, and coordinating the Community's response to all threats with the potential to reach US soil. We think NCTC is a natural fit for this role. (U)

NCTC's Pursuit Group should…

- Focus primarily on threats with the potential to reach the homeland, avoiding the natural temptation to fall back into the traditional, more familiar terrain of focusing mainly on threats overseas.

- Coordinate and deconflict its pursuit of targets with other Community components so that multiple units are not duplicating the efforts of one another.

- Emphasize areas where the Intelligence Community has limited or emerging coverage.

- Develop a coherent set of indicators that will help identify when terrorist groups abroad are adopting a focus on the US homeland; [redacted] (b)(1) (b)(3) ODNI

- Measure success as tapping the full range of US government capabilities to identify and disrupt plots—not by tracking traditional metrics such as production of finished intelligence. ~~(C//NF)~~

CIA and NCTC should…

- Increase the number and frequency of personnel rotations between CTC and NCTC—not just among line analysts, but among senior managers, as well. These should be mandatory and take place with regular periodicity.

- Institute, for all officers, explicit individual performance objectives geared toward jointness and collaboration with the other organization. (U)

All agencies should…

- Encourage rotations and embed their officers in other agencies to improve seamlessness operations throughout the counterterrorism community. (U)

We endorse…

- The DNI's directive on 7 April to formally assign responsibility for the counterterrorism mission, which embodies many of the views we have expressed in the course of our review. In the end, it must fall to leadership and management to marshal the talents of their people and the mandates of their organizations in ways that are mutually reinforcing and that close whatever gaps open up in our counterterrorism coverage.

- The West-Clark panel's recommendations that seek to increase collaboration between FBI and DoD and between FBI and the counterintelligence community. ~~(S//NF)~~

We do not endorse…

- Structural changes suggested by other groups that do not address the root causes of the tension between organizations and may actually complicate the relationship. These include ODNI's recommendation that NCTC lead the PDB planning process on counterterrorism-related stories. We think that exercising current authorities could achieve the same goal—integrated analytic coverage—with less disruption and bureaucratic layering.

- Any division of labor that divides counterterrorism responsibilities exclusively along "tactical" and "strategic" lines. Terrorist organizations do not function that way, nor do analysis and collection. ~~(S//NF)~~

Clearing the Way for Properly Sharing US Person Information (U)

The DNI should work with the Department of Justice to…

- Simplify, harmonize, update, and modify the Community's procedures relating to US Persons.

- Establish a Community-wide, interdisciplinary process for developing guidance and training related to US Persons authorities and procedures and for determining whether new authorities may be needed on emerging issues, such as radicalization, new technological developments, and new forms of terrorist communication. The goal would be to provide clarity and confidence to operators and analysts so that they know how conduct their missions in a way that properly protects privacy and legal interests.

- Institute standardized, continual Community-wide training and guidance on handling US Persons issues. It is especially important that this training and guidance focus on working-level analysts and collectors who are most directly affected by US Persons considerations. ~~(S//NF)~~

The DNI should work with the Community to…

ERROR: timeout
OFFENDING COMMAND: timeout

STACK:

66