Unidentified Male: You're listening to a podcast from the Stanford Center for International Security and Cooperation.

David Holloway: My name is David Holloway. It is my pleasure to introduce this afternoon's panel which will be devoted to a presentation and discussion of the book *Insider Threats,* which has been coedited by two of our panelists, Matt Bunn and Scott Sagan. And Amy Zegart has contributed a chapter to the book. I should say the editors have also contributed chapters to the book. Let me introduce them briefly in alphabetical order.

Matthew Bunn is Professor of Practice at the Kennedy School. He's the Co-PI of the Belfer Center's Project on Managing the Atom. And the focus of his work over the years has been on security nuclear materials and conducting studies that have had a significant influence in defining US policy in relation to nuclear security and on the disposition of fissile material.

Scott Sagan needs no introduction to this audience. He's the former Co-Director of CISAC, the Caroline S.G. Munro Professor of Political Science, and a Senior Fellow here at CISAC and FSI. And his work has ranged widely on nuclear issues with a particular focus on organizational theory to explore issues to do with the safety and security of nuclear weapons and nuclear materials. He heads the global nuclear initiative at the American Academy of Arts and Sciences, Scott? That is still one of your many...

Scott Sagan: I'm still involved in it, but I'm heading their Ethics and War project right now.

David Holloway: Right. And Amy Zegart is the third panelist. And she is the Co-Director of CISAC, a Senior Fellow here and at FSI, and the Davies Family Senior Fellow at the Hoover Institution. She's published three books on American national security agencies and is now leading the program on cybersecurity here at CISAC.

So it would be hard to find a better and more qualified panel to discuss these issues. That's why, of course, they've written the book. So let me turn it over. Scott, I think you're the first speaker.

Scott Sagan: I'll be speaking first. Thank you very much, David, and thank you all for coming. Matt and I have been on the road talking about this book for a while now, speaking at the Department of Energy, the Los Alamos National Lab, the Sandia National Lab, the Livermore Laboratory yesterday, think tanks in Washington, Harvard University, and the American Academy of Arts and Sciences.

But it gives me particular pleasure to come here and speak because this book was actually hatched not just at CISAC but in this room. Indeed, Matt and I had been discussing questions about insider threats for many years since he

and I had had an exchange in the engineering journal Risk Analysis about an article I wrote called "The Problem of Redundancy Problem: How Adding More Security Forces May Decrease Nuclear Security." And what he and I recognized from this more theoretical exchange was that we actually lacked good, empirical work on insider threats.

And as we do here at CISAC, we are able to bring a whole group of people in for a meeting where people present their ideas, and we had engineers, nuclear operators, US Military, Department of Energy people, State Department people, scholars, some of whom like Thomas Hegghammer and Amy Zegart and Jessica Stern had long histories with CISAC. Others were just specialists that we brought in because we really liked the work that they were doing.

And then we commented on each other's work, had a second meeting at the American Academy of Arts and Sciences and decided to take the best papers and try to put them together with Matt and I trying to do a summary. We produced the summary that was also published by the American Academy.

There are many best practices guides about nuclear security. But what we noted was they all talked about really good thing that had happened and very rarely shared the real experiences of all the dumb things that had actually happened that produced the need for all these best practices guides. So with our tongues firmly in cheek, we produced a worst practices guide.

Bismarck once said that only fools learn from their mistakes. Wise men learn from the mistakes of others. And we thought it would behoove us to share stories about things that have gone wrong and try to supply lessons. Many organizations, say diamond mines or casinos, expect that they'll be lots of insider threat problems, theft. There are others that are high security organizations with enormous risk and morale and have a strong sense of loyalty. And we would like to think, and they would like to think, that they don't have insider threat problems. But as we surveyed the field, we recognized that insiders are very common.

Every US Military service, Air Force with Chris Cooke who sold secret launch code information to the Soviet Union during the Cold War. The Navy with John Walker conspiracy theory, again selling material to the Soviets. The Army with Chelsea Manning. Every one of the intelligence agencies has suffered a major insider threat problem with Robert Hanssen from the FBI, Aldrich Ames from CIA, Edward Snowden we all know from the NSA.

And every laboratory that we've been to has had a different insider threat problem, and even at our talk at Livermore, we were just amazed how few people at Livermore knew about their own history of insider threats. We talked about some of the problems that they've had of people caught in relationships with Chinese spies or someone selling information to the Israelis. And that organizational history got lost.

Organizations very rarely like to air their dirty linen in public. What we've discovered is that they very rarely like to air their dirty linen in private, even among themselves. And that restricts now only how much they learn from the past and themselves, but certainly how much they can learn vicariously from each other.

So producing a sense of what are the organizational dysfunctions, what common problems, how common is it for people to see red flags? Whenever we look at an instance, we say oh, boy, how could they not've seen that coming? Red flags are really common when you look at this, and they are ignored at the time. Why is that?

So we came up with a set of lessons. I'm going to walk through the beginning of them, turn it over to Amy who's going to do a deep dive in one of the really superb case studies that she produced for our volume about the Fort Hood shooting incident, turn it back to me. And I'll pass it on to Matt who will walk through the rest of the lessons.

So very briefly, lesson one...and the takeaway I want you to take away is this picture of Indira Gandhi smiling in front of her assassin, Beant Singh. There are death threats against Mrs. Gandhi and her family during the 1984 crackdown on the Sikh uprising. And the individuals involved in the leadership of the security, the equivalent of the secret service, wanted to have extra security personnel and wondered whether it was appropriate to think about restricting Sikhs.

Mrs. Gandhi said absolutely not. We're a democracy. We're multicultural, multireligious democracy. Moreover, my favorite security guard is Beant Singh. He's the one I talk to all the time. He's loyal. They arranged to have more guards, including one of whom was his cousin. They conspired to be put together on a detail. And when they were alone with Mrs. Gandhi, they shot her.

That's very common in organizations to think there are problems of insiders in other organizations but not in our organization. So just as there is a NIMBY phenomenon, not in my back yard, we label this the not in my organization. And to the degree that we can just get people to accept that there are serious problems in all organizations and that their organization is not an exception, we will have done, I think, an important service.

It's especially problematic when you have loyal people who can be converted or can be radicalize or can change. Much of the evidence we see in different case studies that we review in our book show how quickly people turn from being a loyal member of an organization to being an opponent of it.

Here are three examples. And that leads us to conclude that contrary to what

many leaders of organizations, who when you speak to them say we don't have a problem because we've got really good background checks...background checks are not sufficient. They may help sometimes. But there are cases that we know about of people who have learned how to get around background checks, who have learned how to give the right answers or to give misleading answers under lie detection tests. There are loyal employees who are loyal to their organization, like a bank case that we studied, Northern Bank, but they were coerced because they were also loyal to their family.

And this leads us to say that when you have radicalization, you have loyalty, you have all these problems, background checks provide a snapshot. They don't provide a sense of the person's character. It's too often that a leader says I understand my workers. I understand the people because I understand their character. Background checks provide a sense of a snapshot.

Let me turn now to Amy, who will dive deep in one of the most important case studies in our book, that of Nidal Hasan.

Amy Zegart: Thanks, Scott. Let me just say very briefly, these guys are the masters of the incremental commitment strategy. So it was an incredibly enjoyable process to work with Matt and Scott. The whole thing started by saying you can just walk down the hall. Just come to this workshop. It morphed into can you present something, something maybe you're already working on. And now here we are with this book that they've put together.

Let me just also say it takes a community. So parts of this chapter were presented at CISAC. Joe Felter was our discussant. Martha Crenshaw gave me lots of comments. So thanks to all of you for making this project better than it started by a long shot.

I want to talk about the Fort Hood shooting of 2009. So November 5th, 2009, an Army Major named Nidal Hasan walked into the base at Fort Hood in Texas and opened fire. He fired two hundred rounds. He killed thirteen people, and he wounded forty-three. At that time, this was the most serious terrorist attack on American soil since 9/11.

Now Nidal Hasan was not a foreign jihadi who came to the United States. He was a self-radicalized Army Officer who was born and raised in Virginia. He was called Michael by his friends in high school. And he spent his entire professional career as an Army psychiatrist. So the question is what went wrong in this case.

Now initially after the attack, the postmortems, and there were several investigations that started off classified and became more declassified over time. But initially, the postmortems really attributed the attack to leadership failures within the Pentagon, to poor policy guidance, and to political

correctness that possibly prevented officials in the Army from disciplining or taking greater action against a Muslim soldier.

But what I find is that there are organizational weaknesses lurking behind the scenes, both in the Army and in the FBI, that played an essential and overlooked role. Organizational factors, as Scott knows very well and has written so eloquently about, are like the dark matter of the policy universe. They're effecting everything that happens in ways that we often don't realize.

So what I find is that Hasan slipped through the cracks, not so much because individuals made mistakes or feared fallout of political correctness, but because the Army and the FBI operated as they usually did. Structures and processes and cultures designed in earlier periods for rational reasons proved maladaptive to detect this insider threat.

Now let me give you a sense...the criticism always when you have these retrospective assessments is organizations can't be a hundred percent successful. But in this case, it's clear that failure was by no means inevitable. Let me just share with you three reasons why that is.

The first is that unlike some of the other cases in the book, Hasan's radicalization was not rapid. It took place over six years. His transformation from Army Officer to fratricidal terrorist was not sudden, and it was not secret. He was openly radical, and he was flagrantly incompetent at his job.

Just to give you some idea, he justified suicide bombers. He declared his devotion to Sharia law superseded his responsibility to the US Constitution. And he did so to his peers and his supervisors repeatedly over a period of years in conversations, in classroom presentations, in PowerPoint slides, all while barely performing his job. He was rated in the bottom twenty-five percent of his cohort.

One presentation he gave so alarmed his medical residency classmates, they erupted in protest, and the instructor had to stop it after just a couple minutes. Several people reported Hasan to his superiors. This was not a red flag operating in secret. They reported him to his superiors, and two called him a ticking time bomb, which was the title of the Senate Homeland Security Committee report. So this was no secret radicalization.

Now the second picture, many of you recognize this man, he's Anwar al-Awlaki. Hasan appeared on the FBI's radar screen almost a year before he opened fire at Fort Hood because he was discovered emailing Anwar al-Awlaki in Yemen. Al-Awlaki, as many of you know, was a radical American cleric very senior in al Qaeda in the Arabian Peninsula and was later killed in a drone strike in Yemen in 2011. He was also known at that time to be one of the world's most dangerous "virtual spiritual sanctioners," one of the most inspiring terrorist leaders in the world.

So Hasan's first email, the email that trips the wire at the FBI a year before this attack, asks whether a Muslim US soldier who commits fratricide would be considered a martyr in the eyes of Islam. This is the first email that trips the wire. It is the reddest of red flags, and it is the first of eighteen communications between these two men over the next twelve months.

Finally, this is eight years after 9/11, so just to put this time period in context, awareness about the terrorist threat was high at the time, and several reforms, both in intelligence and counterterrorism agencies, had been in place for a period of several years. Failure was not inevitable. So what went wrong and why?

There are two organizations that I look at, the Army and the FBI. And as I'll go through quickly, each suffered from silent organizational deficiencies that made it difficult, if not impossible, to bring these red flags together so that they could sound the alarm and indicate that a trusted insider was becoming, in fact, an insider threat.

Let me start with the Army. I'm going to run through the failures on the left, and then I'll talk about their organizational roots on the right. The Army had essentially three different systems that could have identified Hasan as a growing threat and taken action to prevent that threat. And all three of these systems failed in this case.

The first system is the disciplinary system. Hasan, as I mentioned, was never disciplined. He was never dismissed from the military despite signs of alarming radicalization and terrible job performance. Just to give you a little tidbit about just how bad his performance was, he was an Army psychiatrist who routinely didn't show up for work or answer his phone when he was on call. So despite both radicalization and poor performance, no disciplinary action was ever taken against him.

The second system in the Pentagon was the performance evaluation system used to decide who's going to be promoted. Hasan gets promoted repeatedly throughout his career. He receives positive reviews that the Senate found were no resemblance to the real Hasan. The Officer evaluation reports, which are the forms that are used for promotion, had only one negative grade about Hasan because he failed to take a fitness test during one of his reviews.

The third and final system was the counterterrorism investigatory system, which was run by the FBI but jointly with agency participation from across the US government in organizations called Joint terrorism task forces. So there was a Defense Department official on the Joint terrorism task force that was investigating Hasan.

Now this investigation proved to be slim, to put it mildly. The Defense

Department investigator on the FBI's Joint terrorism task force never interviewed Hasan, never interviewed a colleague, never interviewed a superior. He spent a grand total of four hours on his counterterrorism investigation looking at databases. And he found some of the emails between Hasan and Anwar al-Awlaki, and he concluded that they must be legitimate for Hasan's research.

All three of these failures, if we look more deeply, have organizational root causes. Why was Hasan not disciplined or dismissed from his job? Lots of disincentives to do that in the Army. At this particular point in time, there were extreme shortages, both in terms of rank and in terms of specialty for psychiatrists in the Army.

So there were shortages for Captains and Majors. Hasan was a Captain, then promoted to Major. There were shortages in the Medical Corps. There was a GAO report found that they only had eighty-three percent of the Medical Corps Officers that they needed at the time. And shortages were particularly acute for mental health professionals in the Army. Again, think about the timeframe. We're engaged in two wars with mental health issues skyrocketing within the military. Keeping medical health professionals within the Army was a priority. So there were enormous disincentives to disciplining or dismissing anyone of Hasan's rank or specialty.

One military official who I interviewed for this project told me during that period, everyone was getting promoted. It was impossible not to get promoted. If you suggested it, he said to me, people would think you were stupid.

In addition to this, there were opportunity costs. We all know this in the management world and in the management literature. As one official put it to me, fifty percent of every manager's time is spent managing the three percent who shouldn't be there. And so what the Army did was find a workaround to deal with Hasan. And that workaround is called transferring him to another base. So he left Walter Reed and was transferred to Fort Hood because he was a problem.

The officer who assigned Hasan to Fort Hood told his colleague there, and I quote, "You're getting our worst." Add onto this certainly the incentives that you don't, in particular, want to take disciplinary action against a Muslim given the political considerations at hand, you can see why there were strong disincentives to take action against Hasan.

The second problem, the performance evaluation system. Why was Hasan promoted when we had these red flags that were gathering that were reported to his colleagues and his superiors? Well, what I found is that it's important to understand how these forms are actually used, these officer evaluation reports. They're designed for promotion. They're not designed to catch

insider threats.

They have extreme standardization on these forms, and I got my hands on a copy of one of these forms. And what you see is they have yes no boxes for different criteria. So does the candidate exhibit leadership, yes or no. So the other example I give of this is Stephen Colbert had this very funny segment where he asked mostly Democratic officials whether George W. Bush was a great president or the greatest president to see what they said. So when you truncate the grading range, you can get some pretty weird responses.

And in this case, in the Army's evaluation system, there was literally no room on the form for derogatory information or potential red flags unless you actually wanted to deny that person promotion. So that's why it wasn't in there. So these forms were a poor reflection of reality, but Hasan was not the exception. Hasan was the rule. They were always a poor reflection of reality because of the nature of the form.

Now I just want to add briefly, there's a second evaluation system within the Army at the time that did collect red flags. This is the local personal evaluation system that each commander had for the men and women in his or her unit. But these files were local, and they were temporary. So as soon as someone moved from one command to another, the files were thrown away. So if I were Hasan's commander, I would have no visibility into any of the red flags that anyone had raised at his prior postings.

So you have these formal official forms that don't capture red flags and these temporary, personal, local forms that do capture them but are not aggregating. They're not putting the red flags together. So that's the Army.

Let me turn to the FBI. Two main problems in the FBI, the first is that the Joint terrorism task force investigation worked very poorly. Sorry. I should go back one. I missed one right here, which is the JTTF investigations work poorly. Before I get...I'm going to pile on the FBI in a second.

But the question here is so the FBI investigation I noted concluded that Hasan's emails must be legitimate. Well, why would they make that conclusion? Why would this Defense Official actually come to that conclusion? Well, it turns out, he was the wrong person for the job. What do I mean by that?

Well, it turns out that the investigator on the Joint terrorism task force had no counterterrorism experience, no counterintelligence experience. He came from a unit in the Pentagon called the Defense Criminal Investigative Service, or DCIS, which is charged with investigating waste, fraud, and abuse. I looked and in a two year period, there were only two cases a year where the Defense Criminal Investigative Service dealt with anything remotely connected to counterterrorism or counterintelligence. Perspective is

everything.

So this investigator came to the Hasan investigation and looked at it through a law enforcement lens. He asked whether Hasan had already committed a crime or whether he was in the process of committing a crime at that moment. And the answer was he wasn't. He didn't ask whether Hasan might be a future threat or could be an intelligence danger, a gathering intelligence danger.

The investigator also thought that because Hasan used his actual name in his email communications with Anwar al-Awlaki, it must be legitimate. Because in his research experience, criminals tried to cover up what they were doing and cover up their association and their names. And the fact that Hasan was emailing this radical terrorist with his real name led him to believe that it must be okay, that nothing nefarious was afoot.

So why was this guy investigating Hasan in the first place? Well, because he was from a unit in the Pentagon that was the most expendable, the least mission critical at a moment when we were fighting two wars at the same time. So the FBI asks for people to be detailed to joint terrorism task forces. The Pentagon says who can we spare? Ah, the Defense Criminal Investigative Service, we can spare someone from there. The FBI finds this investigator attractive because like an FBI special agent, he has law enforcement capabilities and authorities.

And so it flies in the face of the whole idea of a joint terrorism task force, which is to bring different perspectives to bear to understand a counterterrorism investigation. Instead, the FBI got more people that treated this investigation like the FBI did, which was a law enforcement investigation.

Okay. So let me now move more explicitly into the FBI. Now the FBI's handling of this investigation within the Joint Terrorism Task Force system was riddled with coordination snafus. There were two joint terrorism task forces involved in this investigation, one in San Diego, which first got the intercept of these emails between Hasan and Anwar al-Awlaki, and one in Washington DC, which had the lead because that's the closest office to where Hasan was working at the time.

So the office that is most concerned about the threat is not the office that's charged with investigating the threat. Each joint terrorism task force then thought the other was doing its due diligence of Hasan's communications with Anwar al-Awlaki, when in fact neither joint terrorism task force was, an example of social shirking in the organization theory literature.

It turns out that after the investigation concluded, there were sixteen more messages between these two men before the terrorist attack sitting in the

FBI's data warehouse system database. Nobody knew they were there because each field office thought the other was tracking them. In these communications Hasan offers Anwar al-Awlaki whatever help he might need, including to call him collect should he be of service. One supervisory special agent in charge of the case in Washington told the FBI's own Fort Hood review, he would've opened a preliminary investigation of Hasan had he seen the additional emails.

In addition to that, there was supposed to be a coordinating mechanism at the FBI Headquarters level in two ways, something called a National Joint Terrorism Task Force, or the NJTTF. The FBI likes its acronyms. And the Counterterrorism Division. Neither one of these organizations provided any coordination role at all. In fact, the National Joint Terrorism Task Force didn't even know about this investigation until after the shooting. So that's the first problem.

The second problem is that the FBI, as I said a moment ago, treated Hasan like a law enforcement case, not an intelligence thread to be pulled. These two problems, again, have organizational root causes. The FBI had coordination snafus because the FBI has for its entire history been a highly decentralized organization with fifty-six different field offices across the United States that operate largely autonomously.

Now this made sense when the FBI was created to have local level priorities driving FBI investigations. It makes much less sense when you're talking about coordination across different geographic ranges to detect and deal with insider threats. So the joke in the FBI is that the FBI is fifty-six field offices with a headquarters attached. That's how weak the central coordinating mechanisms of the bureau are.

And in addition, of course, we have this social shirking phenomenon, which has been found in many other contexts. So the coordination problems shouldn't be surprising given the FBI's history of field office supremacy, left hand no knowing what the right hand is doing.

The second problem, why would the FBI treat Hasan like a law enforcement case as opposed to an intelligence investigation? And the reason here has to do with deep seated structures, incentives, and cultures in the Bureau which has primarily been a law enforcement organization for more than a hundred years. The Bureau always has been law enforcement first, and that means focusing on chasing individual cases and winning convictions.

After 9/11, of course, the goal was to get the FBI to be more intelligence driven. This was a priority of Director Muller who came into office one week before 9/11. And to be intelligence driven, the reforms wanted to get the FBI to collect and analyze intelligence as an end in itself, not just in connection to close a case. But the persistence of that case orientation and agent primacy as

opposed to analysis led both task forces to pick up the right intelligence signals but draw the wrong conclusions.

So instead of searching for intelligence about a connection or implications for the radicalization of Nidal Hasan, they looked very narrowly at the case and whether Hasan was at that exact moment of the investigation engaged in criminal activity. The FBI was not collecting intelligence. It was hunting a criminal, and that's why they didn't find the insider threat in their midst.

I know you all are going to talk about the worst practices guide so I don't want to give that away. But I do want to highlight just a couple of, I think, implications from this particular case. The first is if we look at bullet point number three, even seemingly obvious red flags are sometimes ignored for perfectly rational reasons. There are cost benefit calculations that have to do with careers and structures and incentives that make it highly unlikely that organizations like the Army or the FBI can actually identify, collect, and aggregate red flags. This wasn't a mistake. This is the natural outgrowth of some of these underlying organizational factors.

And finally, if you look at what the recommended policy fixes were after the Fort Hood attack, the Pentagon exhorted leaders to be better leaders. They wanted to promulgate more rules. They disciplined nine superiors in Hasan's chain of command. But when all nine superiors in a chain of command make the same bad call, it's an indication that there are more systemic problems at play. And so these organizational challenges, I find, need more organizational solutions. Let me turn it back to Scott.

Scott Sagan: Great. I'll just give one more example that comes from Jessica Stern and Ron Schouten's marvelous chapter in the book about the anthrax killer, Bruce Ivins, a senior scientist at the US Defense Weapons Laboratory. There are similar and some differences, but some really great similarities in the organizational story that Amy's telling and some also interesting psychological variables that are played up in Ron and Jessica's chapter.

Bruce Ivins is someone who is working on anthrax. He expresses concerns about his own mental health to colleagues. He has conversations with his therapists that leads one of them to say he is dangerous. One of them is so concerned that a junior therapist goes to her boss and says should I warn potential people. He says write it up. I want to see the full report. He ends up getting a long report and decides not to read it because it was too long. There's so much in it that his policy was we wait for a short report. Those are the ones you have to read.

So you should not just assume that red flags won't be read properly. Sometimes they're not even read, R-E-A-D. He had numerous cases of unrequited love from college through his coworkers and became obsessed with a number of these women, would brag about how important anthrax was

and how important it was going to be in the future. He stalked a number of them. One of them did report his behavior and said she was afraid of him to a boss, was afraid that Bruce Ivins might go postal. And she was told, why don't you work in a different part of the lab for a while because he's going to retire soon anyway.

And one of the psychological factors involved here was that Bruce Ivins was a likeable guy part of the time. An affect bias, the psychological effect where if you like one part of somebody and your basic premise is this is a good man, you can overlook so much. And repeatedly we heard the phrase, and they repeat it, among investigators that some of the actions that he was doing was just Bruce being Bruce. He's eccentric.

He's a churchgoer. We like most of his activities, and the idea that this man would decide to spread anthrax, not to create massive killing, just to create enough to create an interest in his own work and to show how important his own work, perhaps to impress the women that he was trying to impress, partly to keep his job for himself to show how important his own work was, was something that people couldn't imagine.

It was only afterwards, after he had tried to cover up his tracks and the FBI was coming down on him that he killed himself, and most of the evidence, I think, firmly points out all these red flags that were ignored at the time. Matt, let me turn it over to you to go quickly through the last lessons.

Matt Bunn: Okay. So in a way, there is an interesting difference in the Bruce Ivins and the Nidal Hasan cases in that I would argue there weren't as many rational reasons for overlooking the red flags in the...but there are always these disincentives. People don't want to get their friends and colleagues in trouble. It's a big pain in the rear end for the reporter because sometimes it's not anonymous reporting and the person knows who reported on them.

I spoke to a person at Y-12 who was working in the highly enriched uranium processing area and was working with a colleague who had a particular very specialized skill in uranium processing. And the guy was starting to act strange, and he reported on him so that person was then taken out of access to HEU for a couple of weeks while they were figuring out what was going on. And the person who reported to boss was like what have you done. You've deprived the organization of these skills. We're going to be weeks behind on our work. Well, you can bet that guy's never going to report again.

So a fourth lesson that we drew is don't assume that it's only going to be one insider. Conspiracies of insiders are possible, and yet a lot of security systems are designed to cope with only one insider, including a lot of nuclear security systems. In one study from Sandia National Lab, they looked at heists from heavily guarded non-nuclear facilities of millions of dollars or millions of dollars in valuables and so on, and found that it was more common to have

more than one insider than it was to have only one insider in the set of heists they were looking at. So where it's practical...it's often expensive, but where it's practical, you ought to design the security system to have at least some capability against more than one insider working together.

A fifth lesson is don't rely on only one layer of security. Some people say oh, I've got portal monitors at the exit that will set off an alarm if somebody's taking out the highly enriched uranium or whatever it is you're protecting. Or I've got searches at the exit. Well, those can all be beaten.

This is a picture of an amazing real life theft from the Antwerp Diamond Center in 2003, which had just an unbelievable security system with many, many layers. But there was a team of thieves, it's really sort of a real life Oceans Eleven kind of situation, that collected intelligence for over two years. They setup a real diamond trading firm so that they could have an office in the building and a safe deposit box in the vault and were going in and out of the vault and observing all of the security for years and then finally ripped off millions of dollars from the vault.

So you need to have a multi-layered system to protect against insiders, and you need realistic testing and rid teaming to try to understand, if you're an intelligent adversary, is there a way you can figure out to overcome this system we've put in place.

A sixth key lesson, and there's a miasma of it around all of the lessons, is don't assume that the culture of the organization doesn't matter or that disgruntlement of employees doesn't matter. Culture of an organization, and whether it's really paying attention to security, not just the security force but everybody in the organization, can be very, very important.

This is not an insider case, but it is an amazing security culture case. This was the intrusion at Y-12 in 2012 where an eighty-two year old nun and a couple of other elderly protesters went through multiple layers of alarmed fences. So they were setting off alarms in a line going directly toward the building with thousands of nuclear bombs worth of highly enriched uranium in it, got right up to the HEU building, were pounding on it with hammers, singing songs, painting on it with blood.

And there were very heavily armed guards inside that building who heard the pounding. And even though it was before dawn and they hadn't been told about any construction that was planned, they said huh, must be construction we didn't know about and didn't bother to go check. Eventually, they were accosted by a single guard.

So why did the guards not respond to all these alarms? It turns out the organization had recently installed a new intrusion detection system, and they had tried to cut corners on the cost of it by incorporating some elements of

the old system into the new system. And that didn't work very well and caused ten times as many false alarms as before to be set off. Normally you would use cameras to check out the false alarms, but the cameras in this area of the site had been broken for months and no one had bothered to fix them. So then the idea was well, we'll send out the guards when there's an alarm. But because there were so many false alarms, the guards had gotten sick of it. And so at that point, you may as well not bother to have an alarm system because nobody's reacting to the alarms. So there was a major breakdown in the security culture at the site.

A good example on the disgruntlement case is the Chelsea Manning case, who's also an issue of emotional disturbance. She was dealing with her dawning recognition of a transgender identity in the middle of the military that was still don't ask don't tell at that time. But she was very bad at her job, similar to Nidal Hasan. She constantly showed up late. And there was a meeting where she was told because of your constant lateness, we're taking away your one day a week off. And she got so angry, she flipped over the interview table and went for the gun rack in the room and had to be restrained. And three weeks later was when she started downloading.

And in a study of cyber sabotage incidents, they found that they were almost always coming after some negative work event like that. A person is denied promotion. A person is reprimanded. A person doesn't get the job they thought that they deserved, and somebody else that they think is less worthy gets it, and then they commit these kinds of insider incidents. And over half of those people were already perceived by others in the organization as disgruntled before the incident occurred, but the organization didn't act on those things.

The other thing that's interesting about disgruntlement is it's relatively easy for organizations to cope with. A lot of organizations had found that pretty simple steps, setting up a sort of employee complaint process where you can go talk to somebody and the person actually listens and validates your complaint and says oh, I'm so sorry you're having that problem and occasionally the organization actually deals with an employee complaint and changes something that employees are complaining about, can greatly reduce employee disgruntlement.

And disgruntlement across a wide range of organizations ranging all the way down to retail stores has been identified as a major, major source of insider threat. When we did this talk in Washington, there's a storied CIA Officer who's not yet fully come out who attended, and he said to me afterward, you're absolutely right on disgruntlement. Almost all the people I've ever recruited, they were willing to betray their organization because they felt their organization had betrayed them first.

So a seventh lesson, don't forget that the insiders may know about the

security system and what its weaknesses are. So this is Robert Hanssen, one of the most devastating spies in US history. And he was a counterintelligence officer. He was the guy who was supposed to be looking for spies. And he was able to monitor the search for the spy inside the organization that was looking for himself and modify his approaches and practices to avoid being caught by that investigation.

Similarly, Edward Snowden, he was an NSA systems administrator. Part of his job was looking for the cyber weaknesses in the system so that they could be patched. We don't know whether the reason he had himself transferred to Hawaii was that he knew that in Hawaii they had not yet installed the network monitoring software to notice unusual activity on the network, but it is true that he had himself transferred there and that they hadn't installed that software there. And so he was able to use very simple tools to download all the huge amount of material that he downloaded without detection.

Another lesson is you can make a lot of security rules. Don't assume everybody's following them. People break security rules all the time. Any one of you who's been in a large organization with a lot of complicated security rules, I'm willing to wager, has violated the security rules at some point. In my own case, for example, I am always late on my trip reports when I do foreign travel. I just don't get around to it. I've got other things going on.

I love this picture. It's an upgraded security door at a Russian nuclear facility upgraded with US assistance and it's propped open. And what's amazing is it's propped open on the day the American investigators were there to take a photograph of it being propped open, which indicates they really didn't get the concept that it was a problem for it to be propped open. But this kind of thing comes up again and again and again and again. The real practice day to day is different from what's in the rulebook.

I hate to gang up too much on my colleagues at Y-12, but this is another example of not assuming the rules are followed. They had allegedly realistic testing of the security system, and the tests were important for the guard force because it affected the size of the bonus payment for the guard force contractor.

And so there was a strong incentive to do well on the test, and they managed to make connections with some of the people doing the testing and get warned ahead of time of exactly when and where and how the adversaries were going to attack, which made it much easier to defend. There are also reports that I think have never fully been confirmed that they were tampering with their laser tag equipment, essentially putting the batteries in upside down, so that being hit with a laser would not be detected. And so the defenders were basically unkillable in the exercises.

A ninth lesson, don't assume that only the consciously malicious insiders

matter. Inadvertent insiders can also be quite important. So this is the jailbreak in a New York prison a couple of years ago. It had never had an escape before, I believe. And there was a conscious insider. But there was also an inadvertent insider who thought he was exchanging things with the inmates to get information about other inmates for better situational awareness within the prison. And he had given them a couple things he thought were innocuous, a couple of small tools, access to this catwalk that they eventually escaped through, and a bunch of hamburger from the conscious insider. And it was a lot of hamburger, and it had hacksaws inside the hamburger.

Inadvertence is a big problem on the cyber front. We all know about clicking on attachments and things of that kind, but these days, the phishing efforts are getting very much more targeted and personalized and so harder to recognize as phishing, especially in the age of social media when it's very easy to find out lots of personal things about you in order to target.

Finally, don't rely only on prevention and assume mitigation doesn't matter. This is not a security incident, it's a safety incident. This is a photograph of the destroyed reactor at Fukushima. But clearly if you'd had some more attention to mitigation, even if you hadn't had the higher seawall for prevention, if you'd had the ability, for example, to get electricity restored, to get water pumped into the cores, you would've been able to avoid having so large a radioactive release.

Similarly, if you think of the Chelsea Manning case, for example, why on earth was a private having access to all the secret cables from all the diplomatic posts all over the world? There's no need for that for that person's job. If Chelsea Manning had only had access to what she needed for her job, there would've been much less damage done.

We have an amazing chapter by Hegghammer and Daehli that provides a lot of interesting data on what jihadists have actually done about nuclear facilities and also what they've written about, not only in publications but even looking into the dark web and so on. And they find actually that there's not a lot there, that jihadis very rarely talk about nuclear issues in general, and almost never talk about nuclear insiders. But we want to have a caveat to the caveat.

First of all, almost all of the real thefts of potential nuclear bomb material, the real sabotages of nuclear facilities, which by the way happens more often than people realize, have been perpetrated by insiders or with the help of an insider, number one.

Number two, jihadists often use insiders in other contexts. So this attack in Afghanistan that killed over a hundred Afghan troops just the other day, there were allegedly four insiders at the base cooperating with the outside

attackers. And there are many other cases.

So I think I'm going to, in the interest of time, skip our sort of positive what should people be doing, and we can get to that in Q&A if people are interested.

Scott Sagan: Why don't you get to the last slide though there. Okay. One last comment before Q&A is that we welcome both questions and comments on our book but especially welcome stories, your own experiences of best practices and worst practices. We have already been collecting a set from other talks that we have given of chapters that we wished we had commissioned and that we may someday commission for others.

Sieg Hecker has told us about his view of the Wen Ho Lee case, the spy in Los Alamos, that he as the director had been told about for over a year before the man was arrested and was told that he could not stop Wen Ho Lee from getting classified information. He had to do nothing to make Wen Ho Lee suspect that he was under investigation because then he might stop stealing things. If he stops stealing things, stealing classified information and taking it home, we might not find out what he's doing with it.

We've heard from Rolf Mowatt-Larssen about the big difficulties of intelligence in the nuclear area when he moves over from CIA to Department of Energy and they have very different cultural views about how to treat insiders and how to treat loyalty.

We've heard from Paul Stockton, our former senior research scholar here, then Assistant Secretary of Defense for Homeland Security, about how he believes that it is very common when you have insider or outsider threats to increase the amount of classified material about them, about all our problems, to say oh, that's the best way to prevent leakage, which means you have to have more people with clearances to do the work, which means the people who give clearances have a disincentive to do them well. It means you have more potential insiders because you add more and more people to the process. Paul's estimate is that there are two million people in the United States now who have secret clearances. That's a real problem.

We add redundancy. We add safety and security. And it can sometimes backfire on us. We very much look forward to questions, comments.

Unidentified Male: You've been listening to a podcast form the Stanford Center for International Security and Cooperation.