AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

[H.A.S.C. No. 112–97]

USE OF AFGHAN NATIONALS TO PROVIDE SECURITY TO U.S. FORCES, IN LIGHT OF THE ATTACK ON U.S. PERSONNEL AT FORWARD OPERATING BASE FRONTENAC, AFGHANISTAN, IN MARCH 2011

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

HEARING HELD
FEBRUARY 1, 2012

U.S. GOVERNMENT PRINTING OFFICE
72–935 WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office,
http://bookstore.gpo.gov. For more information, contact the GPO Customer Contact Center,
U.S. Government Printing Office. Phone 202–512–1800, or 866–512–1800 (toll-free). E-mail, gpo@custhelp.com.

HOUSE COMMITTEE ON ARMED SERVICES

ONE HUNDRED TWELFTH CONGRESS

HOWARD P. "BUCK" MCKEON, California, *Chairman*

ROSCOE G. BARTLETT, Maryland
MAC THORNBERRY, Texas
WALTER B. JONES, North Carolina
W. TODD AKIN, Missouri
J. RANDY FORBES, Virginia
JEFF MILLER, Florida
JOE WILSON, South Carolina
FRANK A. LOBIONDO, New Jersey
MICHAEL TURNER, Ohio
JOHN KLINE, Minnesota
MIKE ROGERS, Alabama
TRENT FRANKS, Arizona
BILL SHUSTER, Pennsylvania
K. MICHAEL CONAWAY, Texas
DOUG LAMBORN, Colorado
ROB WITTMAN, Virginia
DUNCAN HUNTER, California
JOHN C. FLEMING, M.D., Louisiana
MIKE COFFMAN, Colorado
TOM ROONEY, Florida
TODD RUSSELL PLATTS, Pennsylvania
SCOTT RIGELL, Virginia
CHRIS GIBSON, New York
VICKY HARTZLER, Missouri
JOE HECK, Nevada
BOBBY SCHILLING, Illinois
JON RUNYAN, New Jersey
AUSTIN SCOTT, Georgia
TIM GRIFFIN, Arkansas
STEVEN PALAZZO, Mississippi
ALLEN B. WEST, Florida
MARTHA ROBY, Alabama
MO BROOKS, Alabama
TODD YOUNG, Indiana

ADAM SMITH, Washington
SILVESTRE REYES, Texas
LORETTA SANCHEZ, California
MIKE MCINTYRE, North Carolina
ROBERT A. BRADY, Pennsylvania
ROBERT ANDREWS, New Jersey
SUSAN A. DAVIS, California
JAMES R. LANGEVIN, Rhode Island
RICK LARSEN, Washington
JIM COOPER, Tennessee
MADELEINE Z. BORDALLO, Guam
JOE COURTNEY, Connecticut
DAVE LOEBSACK, Iowa
NIKI TSONGAS, Massachusetts
CHELLIE PINGREE, Maine
LARRY KISSELL, North Carolina
MARTIN HEINRICH, New Mexico
BILL OWENS, New York
JOHN R. GARAMENDI, California
MARK S. CRITZ, Pennsylvania
TIM RYAN, Ohio
C.A. DUTCH RUPPERSBERGER, Maryland
HANK JOHNSON, Georgia
BETTY SUTTON, Ohio
COLLEEN HANABUSA, Hawaii
KATHLEEN C. HOCHUL, New York

ROBERT L. SIMMONS II, *Staff Director*
JOHN CHAPLA, *Professional Staff Member*
DEBRA WADA, *Professional Staff Member*
JAMES WEISS, *Staff Assistant*

CONTENTS

CHRONOLOGICAL LIST OF HEARINGS

2012

Page

HEARING:

Wednesday, February 1, 2012, Use of Afghan Nationals To Provide Security to U.S. Forces, in Light of the Attack on U.S. Personnel at Forward Operating Base Frontenac, Afghanistan, in March 2011 1

APPENDIX:

Wednesday, February 1, 2012 33

WEDNESDAY, FEBRUARY 1, 2012

USE OF AFGHAN NATIONALS TO PROVIDE SECURITY TO U.S. FORCES, IN LIGHT OF THE ATTACK ON U.S. PERSONNEL AT FORWARD OPERATING BASE FRONTENAC, AFGHANISTAN, IN MARCH 2011

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

McKeon, Hon. Howard P. "Buck," a Representative from California, Chairman, Committee on Armed Services 1

Smith, Hon. Adam, a Representative from Washington, Ranking Member, Committee on Armed Services 3

WITNESSES

Dahl, BG Kenneth R., USA, Deputy Commanding General for Support, 10th Mountain Division (LI), Fort Drum, New York 5

Motsek, Gary J., Deputy Assistant Secretary of Defense for Program Support Acquisition, Technology and Logistics, U.S. Department of Defense 7

Sedney, David S., Deputy Assistant Secretary of Defense for Afghanistan, Pakistan and Central Asia, U.S. Department of Defense 8

Townsend, BG Stephen J., USA, Director, Pakistan-Afghanistan Coordination Cell, Joint Chiefs of Staff 6

APPENDIX

PREPARED STATEMENTS:

Dahl, BG Kenneth R., joint with BG Stephen J. Townsend, Gary J. Motsek, and David S. Sedney 40

McKeon, Hon. Howard P. "Buck" 37

Smith, Hon. Adam 39

DOCUMENTS SUBMITTED FOR THE RECORD:

[There were no Documents submitted.]

WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING:

Mr. Conaway 53

Mr. Johnson 53

Mr. Scott 53

Page

QUESTIONS SUBMITTED BY MEMBERS POST HEARING:

Mr. Kissell 58
Mr. McKeon 57
Mr. Ruppersberger 60

USE OF AFGHAN NATIONALS TO PROVIDE SECURITY TO U.S. FORCES, IN LIGHT OF THE ATTACK ON U.S. PERSONNEL AT FORWARD OPERATING BASE FRONTENAC, AFGHANISTAN, IN MARCH 2011

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
Washington, DC, Wednesday, February 1, 2012.

The committee met, pursuant to call, at 10:05 a.m. in room 2218, Rayburn House Office Building, Hon. Howard P. "Buck" McKeon (chairman of the committee) presiding.

OPENING STATEMENT OF HON. HOWARD P. "BUCK" MCKEON, A REPRESENTATIVE FROM CALIFORNIA, CHAIRMAN, COMMITTEE ON ARMED SERVICES

The CHAIRMAN. Committee will come to order.

In September last year, this committee explored the issue of attacks by members of the Afghan National Security Forces on U.S. and coalition personnel. The witnesses concluded that the DOD [Department of Defense] had mitigated the risk about to the degree we can in these few occasions when such attacks have occurred.

Since then, the committee staff has continued to look into the factors behind attacks by Afghan nationals on coalition forces, including attacks conducted by Afghans hired by private security contractors to protect U.S. bases.

The staff has used the attack in March 2011 at Forward Operating Base Frontenac as a case study to better understand the range of issues. In that attack, two soldiers died, including my constituent, Specialist Rudy Acosta, and four were wounded.

I would like to note that Specialist Acosta's father and mother, Dante and Carolyn Acosta, are with us here today.

Private security contractors are used in Afghanistan to provide personal protective services for Department of State personnel and dignitaries, to guard construction sites, to ensure safe movement for other private companies doing business in Afghanistan, for guarding supply convoys, and to augment coalition forces by providing base security.

In the case of base security, the Commander in Chief is responsible for determining the size of the U.S. force deployed to Afghanistan and other places around the world, the missions that the force will undertake, and the necessary contractor support.

For different reasons, both President Bush and President Obama have chosen to limit the size of the U.S. force and to use private security contractors to enhance base security.

In contrast, it is Congress' role, and the purpose of today's hearing, to assess the advisability of these policies and whether the administration needs to change its approach.

Complicating matters further, President Karzai has dictated that only Afghan nationals may be certified for employment as private security guards, and has not permitted U.S. citizen contractors.

Karzai has also ordered the private security contractors to be disbanded. The Afghan Ministry of Interior will assume full responsibility for providing the Afghan Personal Protection Force, a new organization that from March 2012 onward, with a few exceptions, will replace private security contractors.

The APPF [Afghan Personal Protection Force] will be available on a fee-for-service basis to coalition forces to perform the services that I just described.

According to the DOD, the Afghan Ministry of Interior, in conjunction with U.S. and coalition forces, will use a vetting and screening process that will be the same for both the Afghan National Security Forces and the APPF.

I recognize that it would be virtually impossible to establish a foolproof screening process. Our own national security screening system is not foolproof.

Yet we must recognize that the existing processes failed to identify 42 attackers from 2007 to 2011. Thirty-nine of those attacks were by members of the Afghan National Security Force and three by contractor employees.

Though less than 1 percent of Afghan forces and security guards have attacked coalition forces, this is 42 attacks too many, and the new process must do better.

Another concern is that the screening and vetting has been tragically weak in picking up signs of threats after the Afghan joined either the Afghan National Security Force or a private security contractor. DOD data indicates that at least 60 percent of all the attacks appear to be motivated by personal matters arising after the hiring.

So it was with the attacker at FOB [Forward Operating Base] Frontenac. In July 2010, at another forward operating base, his employer, Tundra Security, fired him for allegedly making statements about killing U.S. personnel and recommended that he not be rehired.

The contractor's chain of command did not enter that recommendation into the attacker's file, and the attacker was rehired by the same contractor in 2011, just before the attack at Frontenac.

Moreover, because a parallel U.S. investigation of the 2010 allegations concluded that the statements could not be substantiated, the U.S. official at the base decided not to enter the allegations about the attacker in the U.S. watchlist system.

Adding to my concern about the vetting system not being focused in the right place, a U.S. rescreening of all Afghan security guards at Frontenac immediately after the attack resulted in several being dismissed as unworthy of employment.

Finally, I am concerned about the Department's September statement that its efforts have mitigated the risk about to the degree we can. At the time, the committee was not aware that the frequency of these attacks had dramatically increased in 2010 and

2011. In fact, 75 percent of all attacks have occurred in the last 2 years.

The Department attributes the increase with the growth of U.S. forces in Afghanistan. But we need to understand the contributing factors better, so that more effective steps can be taken to further mitigate attacks on U.S. and coalition personnel.

Before introducing our witnesses, I would like to read Mr. Acosta's statement into the record. This was written on Wednesday, February 1st, 2012.

"Last month, we received the U.S. Army A.R. 15–6 report regarding the March 19th, 2011 attack on U.S. Army FOB Frontenac, Kandahar Province, Afghanistan, which resulted in the death of our son, Specialist Rudy A. Acosta and Corporal Donald Mickler, and the wounding of four other soldiers.

The report highlighted the fact that although the U.S. government allows private security contractors to provide base security in hostile lands, basic levels of safeguards were either not implemented or not followed. This allowed an Afghan national, who made prior threats against U.S. troops, to be reemployed by PSC [Private Security Contractor] Tundra Security and carry out a lethal attack.

Our family and the Nation believe that this practice should be ended and rules be put in place so that only U.S. troops guard U.S. troops on these posts. However, as long as this practice continues, these PSCs, like Tundra, must follow rules put in place to safeguard our troops and there must be consequences if they fail to do so.

We are disappointed that we were not allowed to testify in person before the House Armed Services Committee on this critical issue."

I would also inform members that some of the material provided to the committee is classified. The classified items are noted in the hearing memo.

If any member wishes to discuss classified matters after the hearing, our witnesses have agreed to make themselves available in 2337 immediately following this hearing. If any member wishes to go to 2337 for this classified material, please let the committee staff know before our hearing ends today.

Ranking Member Smith.

[The prepared statement of Mr. McKeon can be found in the Appendix on page 37.]

STATEMENT OF HON. ADAM SMITH, A REPRESENTATIVE FROM WASHINGTON, RANKING MEMBER, COMMITTEE ON ARMED SERVICES

Mr. SMITH. Thank you, Mr. Chairman.

I want to thank the chairman for having this hearing, and most importantly for his attention to this issue. I know this has been a huge priority for you and the majority staff and for this full committee. And I appreciate all the work on it because it is a critically important issue.

As you look at the report and see the disturbing number of attacks committed by ANSF [Afghan National Security Forces] and Afghan contractors against our troops, it is indeed a very serious

and troubling situation. Our troops are in Afghanistan to protect the Afghan people and to protect their government.

To be turned on by the very people they are fighting with and for undermines the entire operation, and places our troops at an unacceptable level of risk.

And I think there has been a thorough study of this, but I think it is also clear that we can do more.

More not just in the initial screening process determining who is going to be in proximity to our troops, armed and in a position to cause harm, but even after they are hired, after they have gone through the screening and vetting situation, to continue to monitor for problems and err on the side of interceding sooner, rather than later; that if we are not sure if someone is 100 percent with us and safe, then need to go find them a different job without a gun so close in proximity to our troops and soldiers that places them at risk.

Clearly, there is more screening that could be done and more protection that can be done as we learn more about what motivated these attacks, and hopefully learn and see where those attacks come from.

Certainly, some of them have been infiltration from the Taliban, and we need to make sure we do a better job of screening initially. But a lot of them simply come down to personal matters that arise during the course of their service, but these are things that can be seen by those who are observant.

We need to keep a much keener eye for Afghan National Security Forces and Afghan contractors who may become a problem, and intervene, find ways to protect our troops and put that ANSF soldier who may be a problem in a place where they don't have the proximity to do this kind of harm.

So, I look forward to the testimony, to hear more about what we can do to better protect our troops from these kinds of attacks. And again, I want to thank Mr. McKeon especially for his attention to this issue and for the work.

It is a critically important issue to protect our troops and a major problem right now in Afghanistan.

I look forward to working with our witnesses and the committee to find solutions to better protect our troops in Afghanistan.

And with that, I yield back.

[The prepared statement of Mr. Smith can be found in the Appendix on page 39.]

The CHAIRMAN. Thank you.

Our witnesses today are Mr. David S. Sedney, Deputy Assistant Secretary of Defense for Afghanistan, Pakistan, and Central Asia, from the Department of Defense; and Mr. Gary J. Motsek, Deputy Assistant Secretary of Defense for Program Support, Acquisition, Technology, and Logistics from the Department of Defense; Brigadier General Stephen Townsend, U.S. Army, Director, Pakistan-Afghanistan Coordination Cell, Joint Chiefs of Staff; Brigadier General Kenneth Dahl, U.S. Army, Deputy Commanding General for Support, 10th Mountain Division, Fort Drum, New York.

General Dahl, since you directed the A.R. 15–6 investigation into the attack at FOB Frontenac, we would like you to begin, and then we will just move down the row.

Thank you.

STATEMENT OF BG KENNETH R. DAHL, USA, DEPUTY COMMANDING GENERAL FOR SUPPORT, 10TH MOUNTAIN DIVISION (LI), FORT DRUM, NEW YORK

General DAHL. Chairman McKeon, Ranking Member Smith, and distinguished members of the committee, it is an honor to appear before you.

I welcome the opportunity to contribute to your understanding of the events that took place at FOB Frontenac and I appreciate your oversight of operations in general.

I would like to begin by once again expressing my condolences to the families of the brave soldiers that we lost, and to honor the sacrifices of all service men and women and their families from whom we continue to ask so much.

I am aware that you have previously been provided a full, unredacted version of the Army investigation conducted under Army Regulation 15–6. I am confident that I will be able to cover the key findings and recommendations of that investigation in this open session.

While serving in Regional Command South in Afghanistan, I appointed an officer to investigate the circumstances of the 19 March 2011 attack on FOB Frontenac. In addition to the standard scope of an investigation for any incident resulting in the death of a soldier, we directed this investigation to also specifically consider the role of the security contractor, in this case Tundra, the vetting process to hire local Afghans, and to make recommendations to improve our processes and prevent similar incidents in the future.

The challenges identified in the investigation are complex and the implementation of those recommendations is deliberate and is ongoing. The investigation identified the assailant, a Tundra employee, as an insurgent who infiltrated the ranks of Tundra in order to execute an internal attack.

The attack resulted in the tragic deaths of two great soldiers and the injury of four others. Due to the quick actions of two well-trained soldiers and the excellent response of medical personnel on the scene, the unit did mitigate the impact of this attack and prevented greater casualties.

A key finding of the investigation was that the assailant had indeed been fired months prior for making unsubstantiated threats against U.S. soldiers at a FOB in a different location. Given that the threats were unsubstantiated, neither Tundra nor the command annotated those threats in an official record, which, had they been recorded may have prevented the assailant from being rehired.

Additionally, the investigation revealed that the command found the orders and policies governing the personal security contractor—the vetting and hiring of those, to be vague and confusing. The recommendations from this investigation focused on clarifying pertinent guidance, creating a comprehensive background file for all local Afghan contract hires, and sharing the findings at all levels of the formation and throughout the chain of command to increase awareness and prevent similar incidents in the future.

I will point out that the investigation also made specific recommendations to recognize the courage and quick action of those soldiers who responded to the attack.

The attack on FOB Frontenac was a tragic event. All commanders take very seriously their responsibility to protect our soldiers.

We have taken steps to correct the errors in process and the confusing policies identified in the investigation. But sadly, in this case, these corrections would likely not have altered the outcome.

Nonetheless, it is our duty to explore every avenue to protect our soldiers. And we welcome your leadership and the oversight of this committee, which causes us to examine ourselves and find ways to improve our operations.

Thank you.

[The joint prepared statement of General Dahl, General Townsend, Mr. Motsek, and Mr. Sedney can be found in the Appendix on page 40.]

The CHAIRMAN. General Townsend.

STATEMENT OF BG STEPHEN J. TOWNSEND, USA, DIRECTOR, PAKISTAN-AFGHANISTAN COORDINATION CELL, JOINT CHIEFS OF STAFF

General TOWNSEND. Chairman McKeon, Ranking Member Smith, and members of the committee, thank you for this opportunity to talk to you today about our efforts to assist the Afghan National Security Forces in ensuring their ranks are free from those who might seek to harm our troops, who are fighting alongside them to build an Afghanistan that will never again be a safe haven for terrorists.

First, let me add my personal condolences to General Dahl's for the family of the troops who lost their lives at FOB Frontenac, like the Acosta family who are here today.

I would like to thank them publicly for their son's service and their family's sacrifice.

And to the families of all our troops, both U.S. and allies, who have been killed or injured in other unfortunate attacks like this one during our mission in Afghanistan.

Our bottom line up front is the protection of service members deployed in harm's way against any threat remains one of our highest priorities for our commanders and leaders, both here in Washington and in the field. Although there is no such thing as perfect protection, especially in Afghanistan, we know we must continue to develop effective ways to combat the insider threat to our service members.

To that end, we appreciate this committee's support in exploring the best methods to provide security for Americans and our allies doing the Nation's work in Afghanistan.

As this committee is well aware, our efforts in Afghanistan have not been without great sacrifice. We still face a very determined enemy who uses asymmetric methods to harm our troops, including insider attacks.

A major focus of our military campaign is developing an increasingly self-reliant Afghan National Security Force that can lead the fight in the near future.

We are working closely with Afghan leaders to reduce potential insider threats through a layered system that includes screening and vetting before an Afghan enters service, cultural training for Afghan service members, and growing an Afghan counterintelligence capability so they can detect potential insider threats before they come to fruition.

Now, for our part, we are reinforcing the importance of cultural and language training prior to deployment for our forces, emphasizing the importance of our own conduct each day in reducing unnecessary frictions with our partners, reviewing our own counterintelligence efforts in theater, and finally, reminding our leaders and soldiers they must always have their own protection foremost in their minds and ultimately provide their own security.

One important part of this approach involves an eight-step vetting process that uses both Afghan cultural practices, such as recommendations from village elders, as well as modern technology in the form of biometrics to help screen and vet Afghans before they enter service.

Looking ahead to the transition of private security contractors to the Afghan Public Protection Force, we will see Afghan security guards undergoing a vetting process like this one.

In these brief remarks, I have highlighted some of the efforts to address potential insider threats. As our campaign increasingly transition security lead to the Afghans, and as our role shifts from leading combat operations to a primary focus on security assistance, our military personnel will be increasingly employed as embedded trainers and advisers with Afghan units.

While we can't completely eliminate the potential for insider threats, we can greatly reduce them by using a multilayered approach that includes smart vetting procedures, cultural training, leader and soldier force protection awareness, and counterintelligence efforts.

Again, thank you for your continuous support to our men and women in uniform.

The CHAIRMAN. Thank you.

Mr. Motsek.

STATEMENT OF GARY J. MOTSEK, DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR PROGRAM SUPPORT ACQUISITION, TECHNOLOGY AND LOGISTICS, U.S. DEPARTMENT OF DEFENSE

Mr. MOTSEK. Chairman McKeon, Ranking Member Smith, and members of the committee, thank you again for the opportunity to appear before you to discuss the use of Afghan nationals to provide security U.S. forces in light of the attack on U.S. personnel at Forward Operating Base Frontenac.

I, too, would also like to extend my condolences to the families of our soldiers, and by extension, to all family members who have lost their lives and loved ones. Their deaths are all tragic.

Generally speaking, contractors perform well and provide essential support to the conduct of our operations within Afghanistan. Without them, under the present conditions there, we would have to divert approximately 20,000 troops from essential combat tasks

to perform noncombat-related security functions. And our allies in Afghanistan are in a similar situation.

In other words, we would have to move 30 percent of our force, whose primary mission is to offensively engage the enemies of our Nation, and are equipped and trained for that mission to provide basic security services oriented, primarily, frankly, against criminal elements.

The investigation has clearly shown that although our basic policies are sound, there were weaknesses in execution, and we will continue to address these.

DOD has a broad range of management policies and operational procedures to effect, provide, and achieve more effective oversight and coordination of contractor operations.

Our oversight and responsibilities aren't static, but constantly evolve as we apply insights from lessons learned.

For example, regarding PSCs—and we when we first appeared before this committee regarding the oversight of PSCs, we have gone from a basic memorandum of agreement and the interagency process to a formal DOD instruction.

We are now in the code of Federal regulations. And we are about to finalize an American Standards Institute standard on management and quality. And we will trust that will yield eventually an international standard that we can adopt internationally.

DOD policy requires all contractor personnel, regardless of nationality, to comply with DOD regulations as well as the applicable laws of the United States and the host country. Biometrics is now an integral part of that oversight and vetting process.

Incidents that involve local nationals attacking U.S. forces or allies are unacceptable, and we must do all we can to eliminate or minimize those risks.

Frankly, as the chairman and ranking member have said, I don't believe we can actually fully eliminate them, but we must do everything in our power to minimize them. Because our national objectives in Afghanistan include that our forces work side-by-side with those of the host nation.

I assure you we will continue to assess our procedures and operations to minimize those risks, and improve where we can find and identify shortfalls. There is no end state to the way we review and implement our processes.

Again, the incident at FOB Frontenac was an obvious tragedy, and no investigation or hearing can minimize or relieve that loss.

Hopefully, this testimony provides a documentary baseline of the topics we were asked to address during this hearing. And as my fellow witnesses, we are prepared to address your questions.

Thank you.

The CHAIRMAN. Thank you.

Mr. Sedney.

STATEMENT OF DAVID S. SEDNEY, DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR AFGHANISTAN, PAKISTAN AND CENTRAL ASIA, U.S. DEPARTMENT OF DEFENSE

Mr. SEDNEY. Thank you, Mr. Chairman, Ranking Member Smith, distinguished members of the committee. And thank you for the opportunity to testify today.

I particularly thank you for your continued support for our troops.

It is important in this hearing, and as we discuss Afghanistan, that we focus on why the United States is in Afghanistan. We are there to ensure that Afghanistan is never again used by our enemies to attack the United States.

Our core goal is to disrupt, dismantle, and defeat Al Qaeda, and to prevent Afghanistan from again becoming a safe haven for such attacks.

This is a mission that I know our soldiers, sailors, airmen, and marines understand. Their efforts and sacrifices allow the rest of us to enjoy the benefits of freedom that our military is dedicated to uphold.

The conflict in Afghanistan has and remains a tough war in very difficult circumstances. However, our military has proven immensely adaptable as it has found ways to address those challenges, particularly in the past 3 years.

The changes in the way we fight and partner with the Afghans is key to the success we are having.

Three years ago, we submitted a report to Congress, a 1230 report, saying essentially that we were losing in Afghanistan. Our most recent report demonstrates that clearly the momentum has shifted to our side and the Taliban are on their back foot.

Violence continues to decrease largely due to our close partnership with the Afghans and the Afghan security forces. The more the Afghans take the lead, the less effective the Taliban are.

To a certain extent, the increased partnership may place our force at greater risk, particularly as the Taliban recognized the importance of that partnership and actively attempted to counter it. But partnership also decreases the risk and decreases the need for U.S. and coalition forces to be in Afghanistan over the long term as we move towards on transitioning to Afghan lead and protecting their own country.

I would like to add my sincere and personal condolences to the families of the servicemen who lost their lives, have been wounded in support of these goals, and particularly, I offer condolences to the Mickler and Acosta family and their colleagues for this incident.

Every loss of life is a tragedy, and our military and defense personnel work hard to prevent these incidents and protect our forces. And we also constantly look for ways to learn from past events to prevent further tragedies.

The issue that we are discussing today, that of the insider threat, is larger than this instance of private security personnel killing U.S. service members. In the combat zone that is Afghanistan, similar incidents of violence have occurred, including Afghans attacking our allies, Afghan security forces attacking each other, and Afghan security forces attacking civilians.

Every attack—every event in itself is tragic. And we are working with our allies and partners in Afghanistan and our Afghan partners in order to try to prevent them.

Incidents such as what happened at FOB Frontenac are truly tragic. And as the chairman pointed out, there has been an increase in attacks over the past year, at the same time as we have

surged coalition forces and surged through to the number of Afghan security forces over the last 3 years.

During that time, both our forces, our coalition allies, and Afghan security forces have suffered casualties. And I would add that the number of casualties that we have suffered, and our allies have suffered, and our Afghan allies have suffered is an evidence of the commitment to that core goal that I mentioned before that is shared by all who are involved.

Not all of the insider threat attacks, of course, were caused by insurgent infiltration. In fact, as the chairman mentioned, our studies have shown that the majority are due to other circumstances. Personal issues, combat stress, and other factors, some of which we don't fully understand in every individual case, often underlie these attacks.

Combat stress that leads to use of violence by forces against their colleagues and their partners is something that is an unfortunate characteristic of war everywhere and something that we must do everything we can to prevent in Afghanistan and elsewhere.

However, I want to stress again that partnership with the Afghan security forces is a critical part of our strategy. And that is what is allowing us to make progress in Afghanistan, what is allowing us to have the prospect of transition to Afghan security lead.

We are now in a position where half of the population of Afghanistan is in areas and provinces that are transitioning to Afghan security lead. And the capabilities that they have been able to build through this increased partnership is what is allowing that to happen and allowing the United States, as President Obama has already done, to reduce our presence in Afghanistan by 10,000 forces over the past year.

We have also seen that the attacks on U.S. and our coalition allies by Afghan forces are more likely to happen where there is limited interaction between Afghans and U.S. and coalition forces.

Where there was closer partnership, better interaction, understanding, better mentoring it is less likely that such an attack will occur. We continually need to look at the lessons that we are learning from these tragedies, both the one at FOB Frontenac and more recent ones, to find ways to prevent future ones.

In order to do that, we have to work together with our Afghan colleagues.

As the chairman pointed out in his opening statement, the vetting process for both the Afghan security forces and the follow-on to the security companies of the Afghan Public Protection Force is using vetting methods that we have developed.

It is important that those vetting methods, both the initial vetting and, as the ranking member mentioned, continued vetting once the forces are in place are improved in order to prevent these incidents of attack on friendly forces.

The Afghan Public Protection Force, which the chairman mentioned, is a force that will be under the control of the Ministry of Interior.

As the chairman stated, this is a result of a decree from President Karzai saying that private security contractors, who provide protection to fixed sites, development projects, and convoys, will

transition to Afghanistan lead under the Afghan Protection Force. That will happen for private companies, non-governmental organizations, and other non-military activities this year, and it will happen for military activities in March of 2013, a year from now.

To help build this force, ISAF [International Security Assistance Force] has set up an advisory group which will partner with the Public Protection Force and the Ministry of Interior to develop and train the force. That action is ongoing today in order to have it stood up and ready next month, in March of 2012.

We are also actively looking at ways to improve the Ministry of Interior's ability to oversee the Public Protection Force and the remaining private security contractors that will continue to protect diplomatic activities in Afghanistan.

Vetting is very difficult in a country such as Afghanistan which lacks much of the infrastructure and information systems that we have here. So our vetting process includes use of Afghan traditional methods, such as having village elders provide recommendations on potential recruits, as well as more modern procedures, such as the biometrics that Mr. Motsek mentioned, drug testing and criminal background checks.

In closing, I want to emphasize that we at the Department of Defense take the death or injury of every U.S. personnel in Afghanistan or elsewhere very seriously. The security of our troops and the success of our mission are our top priority.

No system is perfect, but no system, as Mr. Motsek said, is static. We are continually looking at this, and we appreciate the opportunity in this hearing to have your ideas, Mr. Chairman, and those of your colleagues on how we can do a better job.

Thank you.

The CHAIRMAN. Thank you.

As I said in my opening statement, going forward the screening and vetting process must overcome the shortcomings detailed in the AR 15–6 and the other reviews done following the attack at FOB Frontenac.

What corrective actions were taken after the attack at FOB Frontenac and how will those actions and others mitigate the risks inherent in the new screening process?

General TOWNSEND. Chairman, I will take that question. And maybe some of my colleagues will have some additional comment.

There were a number of orders produced after that attack. There was an AAR [After Action Review], just like we always do—Mr. Sedney said we are a learning organization. So, we did an after action review in addition to these investigations, came up with a list of things that we could do better, and fragmentary orders, supplemental orders went out to the force to do that.

Some of those things, specifically, related to some of the weaknesses that were identified in this investigation and a couple of others, specifically, the need for the private security companies to adhere to the same vetting process that we are using with the Afghan National Security Forces.

A couple others that I think were very important were—and Mr. Motsek mentioned this in his opening statement—that we have added a requirement for a weekly screening.

So, they are not just now screened when they first enter service, but there is a requirement for the commanders on the FOBs to screen all local nationals that come on and off the FOB on a random basis at least weekly. That is done through biometrics. So that if new information emerges, there is a chance they will catch that if it wasn't caught when they initially entered service.

A couple other points were made about increasing force protection awareness for our soldiers themselves and their leaders.

I will let General Dahl comment on——

The CHAIRMAN. Let me just ask one question that goes along. Shia Ahmed had gone through the screening, but he had used a little bit different name each time.

And how do you measure that against the biometrics? How do you pick that up?

General TOWNSEND. Yes, sir.

The biometrics—a guy may report in with more than one name, which is not uncommon in Afghanistan, because frequently they have one name and they don't know how to spell it. And it is not clear to us sometimes how to spell it exactly, so it might even be misspelled.

The guy only has one set of fingerprints. He has only got one facial photograph. He has only got one iris scan.

So, it doesn't matter how many names are entered into the biometrics, we are going to know who he is, and we are going to be able to——

The CHAIRMAN. So using the different names—or he could have done that like unintentionally.

General TOWNSEND. That is right. That is right.

Which is not uncommon.

The CHAIRMAN. But the name isn't the important thing. It is the biometrics, how they——

General TOWNSEND. That is exactly right.

And, sir, I will ask General Dahl to speak a little bit more about the lessons learned that were applied in Regional Command South.

General DAHL. Yes, Chairman.

As you saw in the report, we made a number of recommendations as a result of the 15–6 to our higher headquarters to be incorporated more broadly theater-wide, and then across the force, not just in the Army, and also for training.

But specifically in Regional Command South immediately following the approval of the investigating officer's findings and recommendations, in Regional Command South, where we had the authority to implement changes ourselves, we put several things into place.

Our first intention was to close the gap between having people, Afghans, employed on our FOBs that had not been screened. So we set out to put in an order to our subordinate task forces and formations to immediately enroll and screen, as rapidly as possible, all those who are working on those FOBs, so we could control that piece.

The second, sir, was that in a sustainment endeavor, once they were enrolled, we wanted to conduct monthly 50 percent of those working on that FOB would be continually screened at random, 50 percent, against the current watchlist.

So the information had entered the watchlist since they had been vetted initially, there was an opportunity to pick up on that. And it wasn't practical to do 100 percent weekly or monthly, but we chose 50 percent monthly at random against the current watchlist, so that we would have some sustainment mechanism to pick up on new information that would enter.

And then finally, sir, we conducted training. And this was training of our contracting officer representatives, those young officers, in some cases noncommissioned officers, who are responsible for oversight of the local contract in that area, making sure that they were more familiar with their responsibilities, more familiar with the policies and the procedures that the investigation officer had determined were confusing.

I will add, sir, that I am now back at Fort Drum. We still have soldiers who are downrange, and we are preparing others to go. And I had seen some of this incorporated into some of our pre-deployment training as well.

But, again, I can only speak locally in that regard for Fort Drum and RC [Regional Command] South, and 10th Mountain Division.

The CHAIRMAN. Thank you.

General Townsend, why do we need to have Afghan personnel guarding U.S. and coalition bases and soldiers?

What are the implications of having U.S. personnel perform these security missions?

General TOWNSEND. Well, sir, as Mr. Motsek mentioned in his opening statement, this is not a new phenomenon. Our use of contracted security guards goes back a long way in our history, into the 1800s and even before.

And one of the reasons we do that is it reduces the burden on our soldiers, and allows them to focus. We never have enough soldiers. It reduces the burdens on the soldiers and allows them to focus on the primary tasks that they have to do.

As Mr. Motsek said, it is the offensive operations and the complex counterinsurgency tasks that we need them to do. So if they are guarding convoys, or development projects, or fixed sites, or even standing watch on a perimeter, then they are not able to engage in those higher and more complex tasks.

So that is one of the main reasons that we do it, probably the most significant reason that we do it, sir.

The CHAIRMAN. Thank you very much.

Yes?

Mr. MOTSEK. Yes, sir, if I could just say, there is always a misperception that we are using security guards everywhere.

The use of security guards is condition-based. It doesn't relieve the commander in the field for making the determination that this particular location, the threat is more of a military threat as opposed to a criminal threat, and therefore I choose not to use security contractors or eventually the APPF to provide this security.

The commander is not relieved of that responsibility. And so just because we have an installation or just because we have a convoy, that doesn't necessarily mean we default automatically to a contractor-based solution set.

In my opening statement, I mentioned that 20,000 personnel would have to be diverted to this function. But I would also ask,

and the committee is painfully aware of this, that we have a rotational base that we have to use to provide support downrange.

And so generally speaking, the rule of thumb is for every job you have downrange, there are two more in the rear, one who is returned and one is getting ready to go.

So for the 20,000 personnel I was talking about that we presently use in Afghanistan to provide this security process, we would be talking up to 60,000 people in the force, the military force, that would have to be aligned to perform that function.

The CHAIRMAN. Thank you.

Ranking Member Smith.

Mr. SMITH. Thank you, Mr. Chairman.

First, just a question in terms of—security guards are certainly part of the problem, but we also train the ANSF. We train with them, and we fight alongside them.

Of the incidents where they have attacked our troops, I don't know if you know the numbers, how many have been security guard situations where it is people who have been supposedly protecting compounds or protecting areas?

And how many of them have been ANSF forces that were fighting alongside or training with?

Do you happen to know off the top of your head what the breakdown is on that?

Mr. SEDNEY. Three of the cases are involving private security forces. The rest of them are Afghan National Police or Afghan National Army soldiers.

Mr. SMITH. So that seems to be the bulk of the problem in the area.

And I guess the big question I have is, so you go through the initial screening process and obviously it is not perfect. We don't have a 100 percent database on every Afghan national who is signing up to be part of the ANSF or part of these contracting forces, but you do the best you can.

But once they get in there, if there is a concern, a problem—and as you have gone through these cases, I guess two questions.

And number one, have you gone back and found signs in most of those cases where after the fact some of our soldiers or marines have come forward and said, "Well, look, the guy was saying this and doing this. We knew he was squirrely for a long time. We were worried about him."

So have you discovered that?

And second, if you do discover that kind of thing now, what are your options and what do you do? How do you respond?

Do you take this person out of the unit?

How do you respond to those sorts of threats as they become perceived before they actually turn into an attack?

General TOWNSEND. Thank you, sir.

The short answer to your first question is, yes, we have seen signs after the fact. Not in all cases.

You know, we do a pretty deliberate postmortem, the investigations, the AARs. And they sometimes result in soldiers saying, "We saw signs."

Afghan soldiers will say it. Our soldiers will say it sometimes.

In other cases, there is no hint from any witness that there was any trouble with this soldier.

So, once there are signs identified, if someone steps forward and provides those, then the commander there, the contractors and the commanders, can make decisions to remove that individual from the force.

Let us talk about the ANSF in particular.

I was at a FOB in Gardez, Afghanistan, where one day the Afghan intelligence officer came in and briefed the commander that there was a soldier he was concerned about.

And he didn't really have good information. It wasn't really all that substantial.

But the Afghan commander looked at me and said, "He is off this FOB today." And he had him transferred away, just to remove the potential source of the problem.

That is one example of Afghans taking a decision.

Mr. SMITH. And as you have investigated this and learned more about how these incidents happen, have you taken steps in terms of training our troops to, okay, look for this, report it?

I mean, have we upped the awareness in some way, and if so, how?

General DAHL. Yes, sir.

Your question speaks precisely to conducting the after-action report, conducting the lessons learned, and extracting those signals that we weren't attending to previously. And post-mortem when you are conducting these investigations and the soldiers or the Afghans come forward and say, "You know, in hindsight, now it is clear to me that maybe we should have paid more attention to this."

Those are precisely the pieces of information that are incorporated into training so that—and it is spread widely across the formations, so that each soldier, each Afghan is now attentive to those indicators that weren't there before.

So we did incorporate those in Regional Command South locally, and now those are also things that I am seeing in our pre-deployment training for the formations that we are sending in the future.

Mr. SMITH. Thank you.

Thanks very much, Mr. Chairman. I yield back.

The CHAIRMAN. Thank you.

Mr. Wilson.

Mr. WILSON. Thank you, Mr. Chairman.

And thank you all for being here today, also for, Mr. and Mrs. Acosta, our sympathy with you.

I am the father of four sons serving in the military, two who were in combat in Iraq. And so, I particularly have a great sympathy and identification. And I know, too, that our chairman has been deeply affected by your loss.

At this time, General Townsend, I was very grateful. My former National Guard unit, the 218th Brigade of the South Carolina National Guard, served in Afghanistan 2007, 2008, led by General Bob Livingston, who has subsequently been elected the only elected adjutant general in the United States.

But when I went to visit them, because I went every 3 months, I was so proud of their service and concerned.

But it was amazing to me. I thought the 1,600 troops, the largest deployment from our state since World War II, would be concentrated at Camp Phoenix and that the training would be a rotation to the camp.

But to my surprise, our troops were at FOBs and military personnel all across the country. As it turned out, it was, again, such a positive experience that the net of this was that our personnel felt like they were working with Afghan brothers.

So, we know that there can be incidents such as this, and I am just hoping that the persons that I have worked with, that in the future that we are vetting the other persons, the Afghan security forces who are serving.

As we vet, is there any polygraph capability? Or is that used if there is some suspicion of someone being a threat to our troops?

General TOWNSEND. Sir, there is a polygraph capability in theater. However, it is rarely used for this type of thing.

It is a very complex procedure. We rarely employ it in our own security forces here for particular jobs. It is complex and just hard to do on a large scale.

So, I would imagine that polygraph capability could be used in a particular investigation. But we don't typically use it in screening folks for employment, sir.

Mr. WILSON. And I would hope, though, that if a person has been identified as indicating a desire to kill Americans, that that might raise itself to where a polygraph could be used. And with the advances in technology today, I certainly hope that, and whatever biometric records there are, that could be considered.

What is the military standard that is used by personnel to enter unfavorable data about Afghan nationals?

General TOWNSEND. There are a couple of venues for that.

The first—we will just take Afghan soldiers and police, for example.

The first would be with their chain of command through the Afghan system. The Afghans also have a biometric system that we are helping them build and stand up.

And we have our own biometric system. And that biometric watchlist is really a master database of all of our partners, and all of our known and suspected enemies also are in that database.

They are entered into that with their name, and as I spoke about earlier, some of their biological data, identification data, is entered into that.

There is actually a questionnaire that you fill out, address, where you are from, parents' names, all that kind of stuff is entered. And that is probably the best place to put it. That is the watchlist that you hear us refer to.

So if the information is entered into that and uploaded into the database, then all U.S. forces in theater will have access to that information.

Mr. WILSON. And that is very encouraging. And indeed, with the technologies we have today, things that would have been unimaginable can be done.

So, I appreciate that positive response.

I also want to know, what recourse do U.S. commanders have if they are unsatisfied with the Afghan Police Protection Force which has been supplied to a base?

General TOWNSEND. The commanders have complete authority and freedom to secure their unit in any way they see fit. And so if they are any time unsatisfied with any aspect of the security, they are authorized to take whatever measure they need to take to ensure the security of their unit.

Mr. WILSON. And so it could be reported that there is either an individual or maybe a whole unit could be replaced?

General TOWNSEND. Yes, sir.

And in fact, General Dahl can probably speak more about it.

In the specific incidence at FOB Frontenac, there was a new unit that had arrived. And there was in his contractor chain, the perpetrator was identified to be fired.

But in the U.S. military chain, those facts weren't quite as clear. That was a disconnect that we have sought to try to correct.

And General Dahl——

Mr. WILSON. And, General, thank you, I would like to get your point, too.

General DAHL. Yes, sir, two points, to readdress your earlier question.

You were looking for what is the threshold or the standard that would require an entry to be made on the watchlist.

And clearly, we did not have a defined standard to help our contracting officer representatives at the time, which caused some confusion.

And a lot of that is left to the judgment of the individual, which is why we know we have to select the right individual who has the maturity and the training and the expertise to exercise that judgment. And we have to train them.

Those are some of the powerful lessons we learned from this case that we have incorporated.

To your second question, the local commander has the authority to remove anyone from his FOB, from his operating base.

The contractor has the authority to fire. But whether the contractor fires or not, the commander has the authority to remove those people from his base.

And then last, sir, just to reiterate a comment that was made earlier, I don't want to give any impression that military commanders are absolving any responsibility for the security of their soldiers.

These personal security contractors that are hired are integrated into that security plan. And they are placed in those places where they can perform that function and we save our very highly trained, well-equipped, combat-experienced soldiers for the larger tasks.

Mr. WILSON. Thank you very much.

General DAHL. Yes, sir.

The CHAIRMAN. Thank you.

Mr. Reyes.

Mr. REYES. Thank you, Mr. Chairman.

Let me first add my condolences to Mr. and Mrs. Acosta.

Is there—and maybe just a yes or no answer from all four of you—is there a fail-safe system that we could institute that would give us any kind of a guarantee?

General TOWNSEND. Yes, sir, there is a fail-safe system. And I will let my fellow witnesses reply, and I can then explain it a little bit.

Mr. REYES. Okay.

Who?

General TOWNSEND. Okay, sir.

So, the fail-safe system that you are referring to—and we have kind of talked about it here a little bit—is the commander is ultimately responsible for his unit security as are the individual troopers.

And so that fail-safe system that is out there, it is a technique that is employed, is to make sure you post a guard for yourself. And that is always an option to these soldiers.

And they can always post a guard to overwatch what they are doing if at any time they feel the threat warrants it.

Also, there is a technique it is referred to as a "guardian angel." And that is—I guess, a good analogy would be sort of like a designated driver.

The guardian angel is not there to participate in the activity that is being done. He is there to watch out for his buddies while they do that activity, whether it be a meeting, or cleaning weapons, or undergoing physical training.

This guardian angel is prepared to fight. And he is in a position of advantage to overwatch that activity. And that is what he does.

And sometimes that can be done in an unobtrusive way by introducing a person into a meeting who just sits and watches what is going on in the room, and doesn't really participate in the meeting.

So, that is just an example of these fail-safes that are taught to our soldiers in training, and they are available to the commanders and any soldier.

Mr. REYES. Yes, General.

General DAHL. Yes, sir. If I could just—I am not going to disagree with my buddy, but I interpreted your question a little bit differently.

Just to add, we should aspire to develop and implement a fail-safe system. And that is precisely what we are doing, because we are going to meet our responsibilities to secure our formations.

However, we have to remember that in combat environment, not everything turns out the way you expect it. And you simply cannot anticipate everything, and unfortunate events happen. It is a very, very risky environment.

So, we are committed to meet that challenge and do everything we can. But we also have to recognize in that environment we just don't control everything.

Mr. REYES. But if I heard you correctly, this fail-safe system, as much as we can do it—and look, I just want to remind everybody, we had a horrible attack at Khost, right on the border with Pakistan, where we lost a number of CIA [Central Intelligence Agency] personnel.

But what you are saying is that the fail-safe system still requires our military being involved, correct?

General TOWNSEND. Yes, absolutely. And, of course, they are.

And in fact, I didn't mean to imply earlier that—and I thank General Dahl for pointing out that, there is no—I guess, it is probably improper to say there is a fail-safe system, because no system is perfect.

Mr. REYES. Right.

General TOWNSEND. So, this is a thinking enemy that we are dealing with here, a cunning enemy, who wants to hurt us.

And every now and then, the enemy is going to have some success.

So, what we are trying to do is eliminate as much as possible, reduce the possibility that that can happen. But we can't eliminate it completely.

I didn't mean to imply, in any of our statements so far, that U.S. forces don't pull security for themselves. They do.

In fact, again, it is up to the local commanders.

So, there are places where the commanders have made risk assessments that it is appropriate for either local security contractors or Afghan security forces to secure that area.

In other places, they deem that it is more appropriate that we do it together. And in other places, it is very appropriate that we do it ourselves——

Mr. REYES. And if I can just interrupt you, because I wanted to get this other point in.

Do we currently have any backlogs in the system for anyone that wants to know the potential for somebody being a threat? Are there any backlogs?

Are we up-to-date on any inquiries of the system?

General TOWNSEND. Sir, I think I understand your question.

There is actually—it is almost instantaneous if someone wants to check the watchlist. There are some physical limitations to the system.

For example, if I have gone out and enrolled some folks in biometrics, I actually have to go upload it into the master database. And that takes time. It takes resources. And sometimes I have got to have a good signal, a good bandwidth to get my upload out.

So, there are some physical limitations that might be a delay. But we are talking here a matter of hours or days, not a significant backlog to enter data into the database and check the master watchlist.

Mr. MOTSEK. Sir, you bring up an excellent point. This technology helps us do this.

And as General Townsend said, we are managing a bunch of different databases and linking them consistently. But you are all keyed to that piece of equipment down range which has had limited availability, to be blunt about it.

They break. We have challenges.

In light of that—again, trying to improve what we do and recognize what we have learned—next month the Army, for example, will be deploying for the first time.

And, hopefully, we will be deploying in large numbers later this year, a biometric device that is much more simple to operate. It is based on a smartphone technology as opposed to the larger packages that you have seen previous to this.

And we could be much more free in the distribution of those downrange.

So instead of having the existing chains of people providing access, we now give one to the contracting officer representative, him or herself, as opposed to having to go to an intelligence specialist or someone else at the installation.

And that input now becomes multiplied as we proliferate the systems downrange.

Mr. REYES. Thank you.

And thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

Mr. Conaway.

Mr. CONAWAY. Thank you, Mr. Chairman, and also, Mr. and Mrs. Acosta, our condolences, as well.

Fifty-eight percent of these incidences were not related to the enemy we faced necessarily, but would just appear to be personnel disputes between the Afghans and, I guess, somebody, either the Americans or someone else.

The process of maintaining how those disputes are going on and—can you talk to us a little bit about how units are trained to watch for these kind of, for lack of a better place, workplace kind of incidences where somebody gets insulted, or they don't get the job they thought they were going to get, and how do we watch for that.

And then much of that is intuitive based on you were there, you understood what the fight was going on.

How do we hand off in unit rotations, the information about the people who have left there that might be subject to some sort of a workplace issue that could develop into an armed response, so to speak?

General TOWNSEND. Sir, if it is all right, I will take the question about how do we manage the frictions. And I will ask General Dahl to maybe address the question about battle handover of the information.

On your question about the personal reasons, there are a number of personal reasons that cause this kind of a conflict to occur. You pointed out a couple of them yourself.

One of them is just simple insults. Another one is combat stress that the individuals are under.

Cultural misunderstandings, I kind of talked about that in my opening remarks. Those are some of the examples.

Religious and ideological frictions, where I watch you do some activity and I perceive it in one way based on my religion or ideology.

So these are all some of the reasons that go into the personal motivations that these Afghans—when they act out.

Mr. CONAWAY. Looking at the 26 incidences that have happened so far related to that, do we analyze, kind of, what categories those fall into? And can we learn anything from it?

General TOWNSEND. Yes, sir. In fact, we do.

And where we can identify that there are personal motivations, sometimes they are not discernible. Where we can discern those, you can categorize those.

I just described some of the categories. Some of the things we can learn from it, first of all, and I kind of mentioned this in my open-

ing remarks, is the importance of cultural training that all U.S. service members undergo before they deploy.

And in fact, General Karimi, the chief of staff of the Armed Force of Afghanistan, has directed that his soldiers will start undergoing cultural training as well, so they understand a little.

That is not something we have attended to in the past—making sure Afghans know how to deal with us as their partners.

We have been training our side of that equation for a long time.

The other one is our own conduct. Making sure that our own soldiers comport themselves the way we would expect U.S. soldiers to do that.

And I will ask General Dahl if he can talk about, maybe, the transfer of that information about people.

General DAHL. Congressman, two points. One is training, and the other one is leader involvement or leader over watch.

And what we have done, in Afghanistan in particular to get after this, is to insert greater attention to the training and the leader oversight during what we call RSOI, the receiving and the staging and the onward integration of the forces.

So when they arrive into Afghanistan, there is additional attention paid toward the cultural situation in that specific location. Because there are cultural differences as you go from district to district, province to province.

So we will address those so that the soldier is aware and sensitive to cultural differences that could be a problem.

And then also the awareness, but also the involvement of the leadership in that training and in the overwatch is important.

Mr. CONAWAY. Is there specifically in the checklist of handoff from one to—this issue about, here are the five individuals we have had some sort of a dustup with. We don't know if it is going to result in anything.

But I am watching him. You should, as well.

Is there a formal kind of a handoff of that issue specifically between commanders?

General DAHL. Sir at the unit level, the commander-to-commander and his non-commissioned officer 1st sergeant or command sergeant major, command sergeant major, will identify who are the strong soldiers and who are the weak soldiers.

And I think that that applies not only to our own formations but to our partners, as well.

Mr. CONAWAY. Okay, you said you think that applies, but is it institutionalized so that we do, in fact, get some attention paid to this issue, since 26 percent of these incidents occurred not from guys who supported the Taliban or supported Al Qaeda, but are actually just got mad at us for their own reasons.

General DAHL. I understand, sir. I can't say that it has been institutionalized across the Army.

General TOWNSEND. Sir, you make a great point here. And as General Dahl has pointed out, something that a lot of units are doing, but you are asking is everyone required to do it.

Mr. CONAWAY. Right.

General TOWNSEND. I can't answer that affirmatively right now. But I have written it down. We will take that back.

[The information referred to can be found in the Appendix on page 53.]

General TOWNSEND. And if it is not, it is an easy add to the orders that I had talked about earlier.

But is this on the relief in place battle handover checklist that there is a specific point in that relief in place where the outgoing commander and the incoming commander talk about potential insider threats, and people that have been identified as maybe being suspicious will check on that.

If we can get you an answer on that before the end of the hearing we will. But I have written it down to follow up.

Mr. CONAWAY. Thanks. Gentleman yields back.

The CHAIRMAN. Thank you.

Mr. Johnson.

Mr. JOHNSON. Thank you, Mr. Chairman, for holding this hearing on this matter that is critical to the safety and security of U.S. forces in Afghanistan.

I want to also give my personal condolences to the Acostas for the sacrifice that you have made, and the sacrifice that your son made on behalf of this country.

And isn't it comforting to know that that sacrifice was made for the security of a country that you can now come to and petition the civilian authorities to look at the circumstances that led to your son's sacrifice.

You have that ability here in the United States. And that is what your son gave his life for.

And for that we will appreciate him. And we appreciate you for taking your time and resources to petition your government to take a look at these circumstances, to see whether or not there is something that can prevent another family from having to go through what you have had to go through as a result of the same circumstances that resulted in your son's sacrifice.

So, I want to thank you all for being here.

I also want to thank General Townsend and the rest of the folks on the panel today for being here to testify. I cite General Townsend since he is a Georgia native. He is my homeboy.

So, welcome, sir.

I do have a question.

Can you define, General Townsend, what success is in Afghanistan? What would be our success?

And also I would like to know from Mr. Sedney, whether or not we are on course to remove all of our forces from Afghanistan by the end of 2014.

General TOWNSEND. Sir, that question you just asked me is pretty high up on the pay scale for me to answer. But I will just look at our national objectives in Afghanistan as I understand them.

First of all is to ensure that Afghanistan never again becomes a safe haven for transnational—specifically Al Qaeda—but other transnational terrorists that might threaten our country. That is job one on the success list.

Secondly is to do that, we have determined that what we want to do is establish a credible enough Afghan state and security force that they can secure themselves, and we don't have to stay there forever to make sure it is not a safe haven.

So, those are my definitions of success. And I will turn it over to Mr. Sedney to talk about progress.

Mr. JOHNSON. I would also add a comment.

The fact that they, the Afghans, seem to not want us to be there does not mean that they are not interested in protecting their country from outside influence, aka Al Qaeda, or some other terrorist group that seeks to use the country as a base.

Is that correct?

General TOWNSEND. Sir, I would maybe express a little exception to your point of they don't want us there. I have met a lot of Afghans in my three tours there. And there are a lot of Afghans that want us to be there and help them help themselves.

There are certainly a number that don't, but your point is exactly right, and I would agree that just because—even those that don't want us there, don't necessarily want Afghanistan to be a haven for international terrorists.

Mr. JOHNSON. Well, your clarification is well taken.

Mr. Sedney.

Mr. SEDNEY. Thank you, Congressman, and I will certainly fully associate myself with General Townsend's point that we—and your point is accurate as well—we and the Afghans share a goal of having Afghanistan being responsible for its own security.

Afghans don't want their country to be used to attack other countries, with the small exception of those that support the Taliban, which is a very small amount.

You asked if we are on track towards that goal. And I would say yes, we are.

As the President stated in his remarks in June, when he announced that we would be withdrawing 10,000 troops by the end of this year, and we have—by the end of last year, and we did remove those 10,000 troops.

We are on track towards achieving our goal of having an Afghanistan that is capable of defending itself from the threat of terrorism and from the possibility of safe havens.

To do that, there is both a lot of fighting that needs to be done and a lot of training, advising, and assisting the Afghan security forces, because it is building the Afghan security forces through the partnership with them that is enabling that transition to take place.

And already, as I said, almost 50 percent of the country, of the population of the country is in areas that are transitioning.

The Afghans, as General Townsend said, do appreciate the advice and support and assistance that we are giving them, and I would say particularly in the military.

I have met from the top of the Afghan military to the ordinary fighting Afghan, innumerable Afghans who expressed their appreciation for us.

I have heard that from Mr. Wardak, and from the Afghan generals repeatedly, that they appreciate. But that they are also, to be frank, embarrassed by the fact that other countries have to come and do their fighting for them.

They want to do their fighting on their own. We want to enable that.

So, we are on course to do that. And that will enable us to transition to Afghan security lead.

There will be, of course, as the Secretary of Defense has said, a continuing need to train, advise, and assist the Afghan military after 2014, after that transition to their lead.

Mr. JOHNSON. All right. Thank you.

And I am out of time.

If I had more time, I would ask whether this screening process currently used by the Afghan National Security Forces to vet recruits to the Afghan Public Protection Force, whether or not it is adequate and practical. But perhaps someone else will ask that question.

The CHAIRMAN. Gentleman's time has expired.

Will you please take that question for the record?

[The information referred to can be found in the Appendix on page 53.]

Mr. Scott.

Mr. SCOTT. Thank you, Mr. Chairman.

Sir, ma'am, I am sorry about your loss. And I want to thank you for coming today.

I think it elevates the importance of the meeting and reinforces our need to fix the issues over there so that this doesn't happen again.

General Townsend, you mentioned that many times some of the Afghans who are applying for these positions cannot spell their name. One of the things that I was taken aback by when I was in Afghanistan—we were at a NATO [North Atlantic Treaty Organization] police training facility—is the extreme lack of education.

And taking a man or a woman who can't spell their name, or couldn't read a book of the level of *The Cat in the Hat*, if you will, and handing that person an AK–47 [assault rifle] and expecting them to carry out security-related details.

And my question gets back to, in these events that we have seen where we have had these tragedies, is the lack of education a common denominator, or are the attacks carried out by people who—Afghans who may very well be better educated?

Is the education level, has that been a common denominator in the people who have carried out the attacks?

General TOWNSEND. I will ask for General Dahl's help a little bit on the education piece.

I haven't seen any data that associates level of education. I know that we have seen attacks by those who are illiterate, as well as attacks by those who are highly educated.

I don't know. I haven't seen that trend. So, I can't talk to that. Maybe General Dahl can.

I will say that your point about education and literacy is a very important one. And it is something that we are tackling very explicitly.

The NTM–A, NATO Training Mission-Afghanistan, has a very strong literacy program. GIRoA [Government of the Islamic Republic of Afghanistan] has a strong literacy program to—it is probably one of the most important social developments, I think, in all Afghanistan, is there is a very focused program to teach Afghan soldiers and policemen how to read.

Right now about half of the Afghan Army has been exposed to reading between a first and the third grade level. It has been—that target has been ratcheting up.

But the goal is that all Afghan service members in the police or the army during the term of their enlistment, their first enlistment, learn how to read.

And I think this has implications for the country that go far beyond a higher quality security force when they go back to their villages and are able to read after their term in service.

And, General Dahl, can you help me about education.

General DAHL. Yes, sir.

Congressman, thank you for the question.

I would just add that—and you are right.

I was in the South, and in the South illiteracy is particularly high. I learned in my time over there that a lack of education, the lack of ability to read or write or add or subtract did not necessarily limit someone from performing a particular function or achieving a capability.

But it severely challenges our efforts to train them, which—and we learned a lot of lessons about how to go about that in a way where we are communicating more effectively.

It takes a little bit longer. You have to start at a very, very base level.

But I guess we are learning just because someone can't read and write doesn't mean they are not capable, just means you have to go about it a little bit differently.

So, I am not that concerned about that long-run.

I would add that the training program, the literacy program that is part of the development of the ANSF forces is very, very good. It is possible that in the future that cadre of ANSF is—becomes some of the most literate people, at least in the South.

I can say that that would be true. And I will leave it at that.

Mr. SCOTT. I guess my question—and I will end with this and allow this process to move on.

It seems to me that somebody who is less educated would be more susceptible to the rhetoric, if you will, and to be led down the path of carrying out an attack, or some type of terrorist attack by some other type of what they might refer to as a religious leader.

Thank you, gentlemen.

Mr. SEDNEY. Congressman, on that you have asked an excellent question. We will go back and see if there is a connection between illiteracy and training in the carrying out of those attacks.

I don't think we have been asking that question, and based on your input, we will do that.

Thank you.

[The information referred to can be found in the Appendix on page 53.]

Mr. MOTSEK. Sir, if I may add one more thing, with regards to the security contractors.

The reliability of the educated contractor is significantly greater. One of the reasons why we had a fracture early on between the police force and the security contractors is the very good security companies recognized very early if they offered education to their employees, they would have a better and more reliable employee.

Something as fundamental as to be able to count the money you are paid on a given day is extraordinarily important. When you give a person that capability, you have changed something.

Several months ago, when I was in country, I saw a gate guard that I had seen before. He ran up to me and he literally handed me his AK–47.

He handed it to because he read the serial number off the side of it to me. He was incapable of doing that before.

So, I would argue that it is not a question of reliability so much as competency. You have a more competent individual if we follow the path that you have described.

Mr. SCOTT. Thank you.

Mr. Chairman, I yield.

The CHAIRMAN. Thank you.

Last year when I was in Afghanistan meeting with General Caldwell, he pointed out that vast majority of the country are illiterate. And the problem that they have of teaching—a sergeant trying to teach them how to fire a weapon, when he says, "Put four cartridges in," they didn't know what four was.

But he told us at that time that the 70,000 they had recruited that year, most of them had gotten through that training up to the third grade, and vast improvement.

And I think that will have long-lasting effects for the country, too. They felt very good about the fact that they were getting education, and as has been stated, they felt good about that.

Mr. Kissell.

Mr. KISSELL. Thank you, Mr. Chairman, and to the family, thank you for being here today.

We lost a young man in 2010 in Iraq in a very similar situation. It is most troublesome, and our condolences and prayers are with you.

I thank the gentlemen for being here today.

General Townsend, a lot has been said about biometrics. And what happens when the machines don't work?

I read somewhere that there seemed to be a failure and not enough machines throughout the country.

What happens when the machines don't work?

General TOWNSEND. That is a great point, sir, and thanks for that question.

The biometrics is just one piece of a complex and layered system that I talked about in my opening remarks. There are actually four levels to this: prevent, educate, train, and protect. Those are the four levels.

The biometrics comes into the prevent piece. The prevent piece is largely based on that eight-step vetting process.

One step of that vetting process is biometrics. And then you have heard testimony here that we are continuing now with weekly screening.

Mr. KISSELL. And General, if—and I apologize for interrupting. I do want to follow along this path for just a second.

If there was not a machine working in one step for biometrics, checks could not be made. Would that be enough to at least pause somebody being in the process? So, you would not say okay, we

don't have this today, but we will go ahead and bring him in anyway.

General TOWNSEND. And that is a great point. And that is actually one that I think the outcomes of the investigation from the FOB Frontenac incident. And Mr. Motsek can talk about I think, here in a second, the arming process for security contractors.

But no, the process stops when a person can't be biometrically enrolled into the watchlist, his forward movement through the induction process stops.

And if you would talk about arming——

Mr. MOTSEK. Right, as General Townsend said, it has got to be multilayered. And if you follow the procedures correctly, you have the biometric process. And indeed, you have two biometric processes now.

You have the U.S. biometric process and you have an Afghan biometric process that are complementary. So you have got that.

But the same process, you have an arming requirement as well. The Afghan Ministry of Interior is the one who provides you your arming authority from the Afghan government. And we should have the same corollary, and we had the same processes in place where we provide an arming authority as well.

And in this particular instance, as you recall in the investigation, the local commander thought he had a window because this person had been previously employed and the like. He thought he had a window.

My position as the DOD guy is that window does not exist.

You are proper in your assessment that if you cannot properly biometrically enroll someone, if you cannot properly license them to be armed, because that infers training and knowledge on certain rules, that the process has to stop. And then you——

Mr. KISSELL. How complete is the biometric database from all people that are inputting and checking?

How free of stovepiping is this information?

Is it broad, so that various inputs, there is not, say, one department, one country, one unit that is not included or does not have access across the board?

General TOWNSEND. There is an Afghan database and there is a U.S. database. And we share information.

You might understand why we would have a separate database from the Afghans. But by and large, there is not that much difference, but we share information. So, there is a deliberate effort to prevent the stovepiping, sir, that you are talking about.

Mr. KISSELL. Once someone is vetted and once they have been brought in, and I know you talk about the weekly checks, but how difficult would it be, for example, if someone was, say, looked like, if they were Taliban, they looked like someone who had been vetted.

How difficult would it be for somebody else to come on base and assume the identification of somebody who has been vetted?

Do we reach a comfort level? Do we have daily checks?

How difficult would it be for me to come on base looking like somebody else, and have access to be able to do harm?

General DAHL. Sir, I can say, just to refer to my comments earlier.

I know one of the things we did immediately afterwards was to ensure everyone, all of our contractors, not just the personal security contractors, but all of the Afghan contractors on our bases were enrolled and vetted.

But then on a sustainment basis, we went with 50 percent on a monthly basis randomly. That is a case where we would pick on someone like that.

But it is not perfect. We wouldn't pick on them perhaps the day that they walked on and were impersonating someone else, if that is what you are alluding to.

And really it is a material solution. It is how much time and how much equipment do you have to dedicate to this.

So again, we want to aspire to the perfect solution, given the limitations that we have. And those are the measures that we have taken.

Mr. KISSELL. Thank you, gentlemen.

Thank you, Mr. Chairman.

I do have some other questions that I will forward for outside follow-up.

The CHAIRMAN. Thank you.

Mrs. Hartzler.

Mrs. HARTZLER. Thank you, Mr. Chairman, thank you, panel, and most of all, thank you for coming today, for your service and your sacrifice.

Our prayers are with you and the Nation's gratitude. So thank you, thank you.

Regarding the incident, I want to kind of hone in on that a little bit. And it looks like, that first of all, the Tundra employees did an investigation and let this person go.

But that recommendation was never incorporated into the Tundra personnel records. And then subsequently, the U.S. investigated also into the allegations, but they couldn't substantiate the credibility of the statements, so the officer decided not to enter this information in.

I would like to know, since this happened what change of procedures has there been, first of all, in U.S. policy at it relates to investigations of this kind?

If they determine that somebody is unsubstantiated, then what is the process?

Has that been changed? Or are they required now to enter that? Or——

General DAHL. Ma'am, I will start, and then I will hand it off.

You are correct. Your read of the investigation is exactly correct.

We had two different judgments that were made, one by the Tundra contractor, one by the officer who was responsible. And it speaks to the question that was raised earlier as to what is the threshold that would require a mandatory entry in there.

I know that what we did afterwards locally was to essentially raise that threshold, raise any suspicion, that would cause an entry to be made and that person to be removed.

And this partly explains why post the attack at FOB Frontenac, when we went and did that vetting of all the employees there, that some additional ones were removed.

I will ask my colleagues if they could talk about how we have institutionalized that beyond my experience.

General TOWNSEND. I think it was Ranking Member Smith, who said earlier that we need to intercede earlier. If it is unclear, err on the side of safety, which I think kind of sums up what we are talking about here.

But in the end, these are judgments by leaders and commanders on the battlefield.

So if someone brings an allegation to me, I am going to hear it out and explore it. And at some point, I will make a decision that it is either substantiated and he is fired, or it is substantiated and he is fired or he is not fired, but it is put as a note in the watchlist.

Or it is completely unfounded because this guy has got some—there is some conflict between the two of them. So, the person who is giving me the allegation is just unfounded. And so, I might make a decision not to enter it.

Just because an allegation has been made, these leaders out there are making those judgment calls.

But I think Mr. Smith's point about err on the side of safety for the U.S. soldiers is a good rule to go by, ma'am.

Mr. MOTSEK. The other thing that changed was that—again in the investigation, because it was unsubstantiated, the senior leadership of Tundra chose not to put it in the person's file.

We now require them to put "investigation concluded, it was unsubstantiated," so it is not a non-response. It is not a non-placement. You have to make an affirmative decision, and record that affirmative decision now.

Mrs. HARTZLER. I am glad to hear that.

General TOWNSEND. Can I add?

One of my assistants here just handed me a note that says actually the USFOR–A [United States Forces–Afghanistan] order requires an entry to any incident that may pose a threat to U.S. personnel such as threats, if the person makes a threat or has a negligent discharge with their weapon.

But again, there is going to be some line there where it is a commander's call. Is that really a threat or is that not?

And that is what we are talking about.

Mrs. HARTZLER. Okay. I am a little confused as to what you just said.

I thought you just said that it is procedure that it is entered. But then you say, it is up to the commander's call. So is it or isn't it?

General TOWNSEND. Yes, such things, obvious things such as threats. So if I make a threat against an American force, they are required to enter.

But if someone says, "I heard so-and-so make a threat to an American force," there is going to be a commander who is going to investigate that, and he is going to make a decision. "Okay, I don't think that is credible."

Is it credible or is it not credible?

If I know that he threatened Americans, that is very credible.

General DAHL. And, ma'am, just to tie it back to the investigation also, the officer who did not enter that in there determined that the threat was unsubstantiated. So, he was not required to make an entry at that time in his judgment.

Had he made the judgment that it was a substantiated threat, he would have made the entry.

Now, it is a requirement to make that entry. But still there is a judgment that has to be exercised as to whether or not this is a credible threat, or if this is just someone who is—it is a family dispute and they are trying to cause problems for another.

Mrs. HARTZLER. So, you say he does have to enter it, though, even if he doesn't let him go, he does enter it?

General DAHL. Yes, ma'am. The policy requires the entry be made if the judgment is made that he is a threat.

Mrs. HARTZLER. Got you. I think that is good.

It needs to be in there, even if it is unsubstantiated. People need to know.

And I want to follow up on your earlier anecdotal story about the Afghan security officer.

General, you said they came in and there was a soldier and they had some concerns about them, so they let him go and moved him out of that.

What was done with him, besides just letting him go? I am a little concerned he might go to another FOB and do the same thing.

General TOWNSEND. Right. In the case that I was referring to, that soldier had a personal conflict—reportedly had a personal conflict with a specific American soldier, not that he had a problem with all Americans.

But there was a personal insult that was perceived by this Afghan soldier. And so the Afghan commander made a decision to move him away to a different location and remove him from that conflict.

At the time, I thought that was an appropriate decision made by an Afghan leader dealing with an Afghan soldier.

Mrs. HARTZLER. But hopefully note that conflict in his record that went with him. Yes?

General TOWNSEND. I don't know about that at the time, ma'am. This is about a year and a half ago. And even at that time, all of our Afghan security forces weren't yet entered into biometrics.

Mrs. HARTZLER. I appreciate it. I just think we need to err on the side of caution and have a valid record that goes with people so that in the future people know of past instances to avoid any potential future negative incident.

Thank you. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

Mr. Platts.

Mr. PLATTS. Thank you, Mr. Chairman. Appreciate your holding this important hearing. Certainly appreciate all the witnesses' testimony and focus on this important issue.

I want to add my words of personal sympathy and gratitude to the families who have lost loved ones.

You know, we can often take for granted the freedoms we have, and the truth is, we only have the blessings of freedoms we do as Americans because of heroic selflessness of our men and women in uniform who are willing to go into harm's way and give their lives in service to this Nation.

So, we certainly have you in our prayers, and our gratitude for you giving your loved ones for all of us.

General Townsend, if you could comment—and I recognize we are in an open setting here, not a classified setting—but earlier today, Reuters reported the following: "The United States military said in a secret report that the Taliban, backed by Pakistan, are set to retake control of Afghanistan after NATO-led forces withdraw, raising the prospect of a major failure of Western policy after a costly war."

Again, knowing we are in an open setting, are you able to comment at all on the existence of this report, or the general characterization about the Taliban retaking control, anything in your knowledge that would relate to what is being reported today by Reuters?

General TOWNSEND. I can comment a bit about it, but, as you said, not much because of the classified nature of the report.

Mr. PLATTS. Understood.

General TOWNSEND. The truth is I am aware of the existence of the report. I have received a copy of it. But I haven't read it and digested it myself.

What I do know is the report is taken from interrogations of Taliban prisoners. And so, these guys that were—you got to keep it in context.

The folks that are quoted in this report are some of the most ideologically committed folks on the enemy side. So, I don't think they are representative, one, of the Taliban as a whole, nor are they representative of the Afghan people.

I think that is probably—best I know off of a quick glance at the cover of the report, that is about all I can say on it.

Mr. PLATTS. So based on your knowledge and what we can talk about here in an open setting, the report isn't a finding of our own intelligence gathering out there on the street, in essence, but more those who we have captured who are in a defiant manner saying this is what is going to happen.

And so the credibility of the basis of that report needs to be maybe closely scrutinized?

General TOWNSEND. I don't want to attack the report because I haven't read it. But I just want to keep it in context, that the reports are coming from enemy soldiers held in captivity——

Mr. PLATTS. And maybe say the credibility of the source or the basis of the report, not the report itself.

General TOWNSEND. Yes, sir.

Mr. PLATTS. Okay. Thank you.

And, again, appreciate all of our witnesses for your service to our Nation. And we are grateful for what you do.

So, Mr. Chairman, I yield back.

The CHAIRMAN. Thank you very much.

I want to thank you for being here today. I appreciate the testimony that you have given, the questions that have been asked.

I believe we have received some of the answers that we have sought on how we can reduce the number of these attacks.

The committee will continue to review and investigate these attacks and work with the DOD to constantly work on making improvement in this area with the DOD and with the Army.

Thank you very much.

This hearing then is adjourned.

[Whereupon, at 11:40 a.m., the committee was adjourned.]

A P P E N D I X

February 1, 2012

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

FEBRUARY 1, 2012

Statement of Hon. Howard P. "Buck" McKeon

Chairman, House Committee on Armed Services

Hearing on

Use of Afghan Nationals To Provide Security to U.S. Forces, in Light of the Attack on U.S. Personnel at Forward Operating Base Frontenac, Afghanistan, in March 2011

February 1, 2012

In September last year, this committee explored the issue of attacks by members of the Afghan National Security Forces on U.S. and coalition personnel. The witnesses concluded that DOD had "mitigated the risk about to the degree we can," in "these few occasions" when such attacks have occurred.

Since then, the committee staff has continued to look into the factors behind attacks by Afghan nationals on coalition forces, including attacks conducted by Afghans hired by private security contractors to protect U.S. bases. The staff has used the attack in March 2011 at Forward Operating Base Frontenac as a case study to better understand the range of issues. In that attack, two soldiers died, including my constituent, Specialist Rudy Acosta, and four were wounded. I would like to note that Specialist Acosta's father and mother, Dante and Carolyn Acosta, are with us today.

Private security contractors are used in Afghanistan to provide personal protective services for Department of State personnel and dignitaries, to guard construction sites, to ensure safe movement for other private companies doing business in Afghanistan, for guarding supply convoys, and to augment coalition forces by providing base security. In the case of base security, the Commander in Chief is responsible for determining the size of the U.S. force deployed to Afghanistan, the missions that force will undertake, and the necessary contractor support. For different reasons, both President Bush and President Obama have chosen to limit the size of the U.S. force and to use private security contractors to enhance base security. In contrast, it is Congress' role, and the purpose of today's hearing, to assess the advisability of these policies and whether the Administration needs to change its approach.

Complicating matters further, President Karzai has dictated that only Afghan nationals may be certified for employment as private security guards and has not permitted U.S. citizen contractors. Karzai has also ordered the private security contractors to be disbanded. The Afghan Ministry of Interior will assume full responsi-

bility for providing the Afghan Personal Protection Force (APPF), a new organization that from March 2012 onward, with a few exceptions, will replace private security contractors. The APPF will be available on a fee-for-service basis to coalition forces to perform the services I just described.

According to DOD, the Afghan Ministry of Interior, in conjunction with U.S. and coalition forces, will use a vetting and screening process that will be the same for both the Afghan National Security Forces and the APPF.

I recognize that it would be virtually impossible to establish a foolproof screening process. Our own national security screening system is not foolproof. Yet, we must recognize that the existing processes failed to identify 42 attackers in 2007 to 2011. Thirty-nine of those attacks were by members of the Afghan National Security Force, and three by contractor employees. Though less than one percent of Afghan forces and security guards have attacked coalition forces, this is 42 attacks too many and the new process must do better.

Another concern is that the screening and vetting has been tragically weak in picking up signs of threats after the Afghan joined either the Afghan National Security Force, or a private security contractor. DOD data indicates that at least 60 percent of all the attacks appear to be motivated by personal matters, arising after hiring.

So it was with the attacker at FOB Frontenac. In July 2010 at another forward operating base, his employer, Tundra Security, fired him for allegedly making statements about killing U.S. personnel and recommended that he not be rehired. The contractor's chain of command did not enter that recommendation into the attacker's file, and the attacker was rehired by the same contractor in 2011, just before the attack at Frontenac.

Moreover, because a parallel U.S. investigation of the 2010 allegations concluded that the statements could not be substantiated, the U.S. official at the base decided not to enter the allegations about the attacker in the U.S. watch list system.

Adding to my concern about the vetting system not being focused in the right place, a U.S. rescreening of all Afghan security guards at Frontenac immediately after the attack resulted in several being dismissed as "unworthy" of employment.

Finally, I am concerned about the Department's September statement that its efforts have "mitigated the risk about to the degree we can." At the time, the committee was not aware that the frequency of these attacks had dramatically increased in 2010 and 2011—in fact, 75 percent of all attacks have occurred in the last 2 years. The Department attributes the increase with the growth of U.S. forces in Afghanistan. But, we need to understand the contributing factors better, so that more effective steps can be taken to further mitigate attacks on U.S. and coalition personnel.

Statement of Hon. Adam Smith

Ranking Member, House Committee on Armed Services

Hearing on

Use of Afghan Nationals To Provide Security to

U.S. Forces, in Light of the Attack on U.S. Personnel

at Forward Operating Base Frontenac, Afghanistan,

in March 2011

February 1, 2012

Thank you, Mr. Chairman, for calling this hearing. I would like to thank our witnesses for agreeing to come before us to testify about this subject as well.

We ask our brave men and women in uniform to take on many risks and dangers in wartime, and they should not have to be concerned about being attacked by those whom they serve with or seek to protect.

We in Congress, and those in the Pentagon, owe it to our military personnel to do everything we can to reduce this sort of risk. Like the actions taken over time to reduce friendly fire casualties, eliminating the threat of "insider attacks" should be a high priority, whether from a private security contractor or member of the Afghan National Security Forces (ANSF). Hearings such as the one today are helpful in determining what drives these sorts of attacks, and what policymakers can do to prevent them from occurring in the future. It is our duty to do whatever we can to protect our men and women in uniform, and that includes preventing attacks from the Afghan troops that they serve with.

In addition to presenting a security risk to our troops, attacks of this nature also undermine the trust between U.S. and Afghan personnel. That trust is a key ingredient in our efforts to build the ANSF, and those forces are a key factor in our plan to eventually wind down our involvement in the war in Afghanistan. Similarly, if our military personnel cannot rely on those hired to guard U.S. bases, they cannot be effective.

Again, I would like to thank our witnesses for appearing today and thank the Chairman for holding this hearing.

STATEMENT BY

DAVID S. SEDNEY
DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR AFGHANISTAN, PAKISTAN, AND CENTRAL ASIA

GARY J. MOTSEK
DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR PROGRAM SUPPORT

BRIGADIER GENERAL (PROMOTABLE) STEPHEN J. TOWNSEND
DIRECTOR, PAKISTAN-AFGHANISTAN COORDINATION CELL

BRIGADIER GENERAL KENNETH R. DAHL
DEPUTY COMMANDING GENERAL FOR SUPPORT
10TH MOUNTAIN DIVISION

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE
U.S. HOUSE OF REPRESENTATIVES

USE OF AFGHAN NATIONALS TO PROVIDE SECURITY TO U.S. FORCES

SECOND SESSION, 112TH CONGRESS

FEBRUARY 1, 2012

Updated 1/31/2012 8:21 PM

Chairman McKeon, Ranking Member Smith, and distinguished members of this Committee, it is an honor for us to appear before you today.

Today's testimony will answer the questions posed in the Committee's January 17th letter to Secretary Panetta, specifically the findings of the investigations conducted in connection with the attack at Forward Operating Base Frontenac; the current screening and vetting process for the Afghan Public Protection Force, and the broader policy questions related to the use of Afghan nationals to provide security for U.S. forces. It is our understanding that the Committee has received the documents referenced in the following testimony.

We would like to begin by recognizing the great sacrifice of our service members supporting our military mission in Afghanistan, to include those who lost their lives during the March 2011 attack on Forward Operating Base Frontenac. The protection of our service members serving in contingency environments such as Afghanistan remains a high priority for Department of Defense leaders and our commanders in the field. We always strive to implement the best systems and practices possible to protect our soldiers, while recognizing there is no such thing as perfect protection. We continuously review our force protection posture and strive to improve and develop the best methods to counter insider threats. The Department of Defense appreciates the Committee's interest and support in addressing the best methods to provide security for U.S. personnel deployed to Afghanistan.

Context

The insider threat is an issue of increasing significance to coalition forces and Afghan National Security Forces (ANSF) operating in Afghanistan. It creates distrust between our forces and their Afghan counterparts during a critical juncture in Afghanistan. It is essential that we work closely with the ANSF to implement a multi-layered defense that includes comprehensive vetting procedures, cultural awareness, unit and leader force protection awareness, and counterintelligence efforts in order to protect our forces.

The insider threat includes both actions by insurgents and ANSF members, whether a rogue Soldier or individual of authority, and can be categorized as: Co-option, Infiltration, Impersonation, and Personal. If for some reason, such as a significant lack of evidence, an incident cannot be categorized, it is labeled as unknown. Likewise, any "green-on-blue" attack investigations still pending results are categorized as unknown. The definitions for each category are listed below.

- ***Co-option*** occurs when an existing ANSF member is recruited to assist or act on behalf of the insurgency. A member can be recruited through multiple means, and it allows the

insurgency to access the ANSF, but unlike infiltration, co-opting an existing ANSF member circumvents the initial screening and vetting process to which new recruits are subject.

- ***Infiltration*** transpires when an existing insurgent member clandestinely joins the ANSF through the standard recruitment process in order to support the insurgency. Although it is difficult to quantify levels of infiltration or verify individual cases as infiltration, there is likely some degree of infiltration that has occurred within the ANSF. One factor in the difficulty of proving infiltration is that the infiltrator is apt to remain undetected. A successful infiltrator is more likely competent and experienced and may be used in a more tactically effective manner, such as facilitating insurgent efforts by providing intelligence on coalition force tactics or movement, or by targeting high-profile ANSF or Afghan Government officials.

- ***Impersonation*** occurs when an insurgent poses as an ANSF member to conduct attacks. With counterfeit uniforms and IDs available, impersonation is often easier to accomplish than co-option or infiltration. Insurgents are increasing the use of the tactic of wearing ANSF uniforms while conducting attacks.

- ***Personal*** is defined by the ANSF member acting intentionally yet independently as an individual perpetrator without direct guidance, command, or preplanning from external entities. These attacks account for the majority of "green-on-blue" incidents, or attacks by friendly forces on U.S. forces, as attackers are spurred by personal motivations, grievances, or emotions and may act with some premeditation or it may be a spontaneous action. Personal motivation assessments can be further subcategorized into ideological, combat stress, and unknown. Ideological indicates that the individual was motivated primarily by a desire for jihad, intended to kill coalition forces to become a martyr, and/or is backing the cause of the insurgency ideology. Combat stress encompasses a variety of conditions that push the individual to the breaking point and cause him to act out, such as a cultural misunderstanding, a lack of appropriate emotional intelligence, depression or stress from combat operations, drug use, or personal grievances.

International Security Assistance Force (ISAF) reporting indicates that 42 green-on-blue events involving ANSF personnel and three (3) involving private security companies (PSC) personnel have occurred since May 2007. These attacks resulted in the deaths of approximately 70 coalition personnel and approximately 110 wounded. We assess the majority of insider attacks resulted from the personal motivation of the attacker. The second most prevalent causes of insider attacks were impersonation and infiltration, with co-option attacks assessed as the least common. Some events remain undetermined because they are pending results of an ongoing investigation. The preferred method of insider attack was the use of small arms fire.

The Perpetrator

The commanding general for Regional Command - South (RC-S) directed an Army Regulation (AR) 15-6 investigation into the March 19, 2011, attack at Forward Operating Base (FOB) Frontenac, which resulted in the death of two U.S. Soldiers and the wounding of four others. The AR 15-6 investigation report, which has been provided to the Committee, discusses the assailant and the information that was known about the assailant at the time of the attack.

Tundra Contractor

At the time of the FOB Frontenac incident, Tundra was contracted to provide security at nine (9) installations in Afghanistan. Pursuant to the terms of its contract, Tundra was required to submit a plan detailing its processes for hiring employees, performing background checks, and providing the results of the background check to the contracting officer for review and acceptance.

The plan submitted by Tundra required agency checks at both the local and national level. Local agency checks included identity verification via valid Tazkera (the Afghan identity card), verification of work history, address confirmation, fingerprinting, and a local police check to receive a clearance certificate for each employee. National agency checks required the contractors to submit a completed employee information package to the Afghanistan Ministry of Interior (MoI) and the Afghanistan National Directorate of Security (NDS), which investigates major crime and potential connections to terrorist organizations. Pending a successfully cleared background check, the Afghanistan Ministry of Foreign Affairs would then issue a certificate of successful vetting and acceptance.

Additionally, Tundra was required to support the Afghan Government (GIRoA) portion of the vetting process by submitting requests for biometric enrollment, ensuring the availability of language interpretation services during the screening and enrollment processes, and requesting Global Unique Identification number from GIRoA enrollers to verify each individual enrollment.

Prior to submission of an arming request, all local nationals and third-country nationals must submit to full biometric enrollment. Additional routine biometric screening then continues in accordance with local installation policies and procedures. Like all contractors, Tundra is required to immediately notify the contracting officer's representative, the local installation Force Protection agency, and the theater arming approval authority of individuals who are revealed as potential security risks during biometric processing.

Tundra was also required to develop a process by which employee termination would be communicated to the contracting officer and local installation Force Protection agencies. While

the aim was to prevent unauthorized access, the process also communicated potential security risks to NDS for biometric watch list consideration. To prevent the rehiring of high-risk personnel, all contractors were additionally required to develop a plan of action to address the tracking and communication of employee dismissals to all sites managed by the contractor. Finally, according to the terms of its contract, Tundra was required to maintain records on the screening status of its employees for six months following termination.

Tundra's record for biometric enrollment is, and has been, significantly higher than the Combined Joint Operations Area - Afghanistan (CJOA-A) average. Tundra's biometric rate was 94.9% in March 2011 and 95.4% in January 2012, as compared to the CJOA-A average of 80.1% as of January 2012. ACOD is working with individual PSCs to identify employees who have not completed biometric enrollment; and, since November 2011, ACOD has also provided this information to the appropriate contracting agencies to support biometric compliance.

If, in spite of the vetting and screening process, Tundra identified an employee as a credible threat, they would have been required to identify the individual to the contracting officer's representative, the contracting officer, and the local installation Force Protection Agency to prevent unauthorized access and to ensure the employee's disposition was included with his biometric enrollment data.

Tundra's official records did not indicate that the perpetrator of the FOB Frontenac attack was terminated because he posed a threat, since the allegation was investigated and determined to be unsubstantiated. Subsequently, Tundra did not inform U.S. military authorities that he was considered a threat. He had been biometrically enrolled during his previous term of employment with Tundra, but had not yet been re-enrolled at the time of the incident, although a request for re-enrollment had been submitted.

In response to the incident, and in coordination with Task Force (TF) SPOTLIGHT and Senior Contracting Official - Afghanistan (SCO-A), the Defense Contract Management Agency - Afghanistan (DCMA-A) conducted a comprehensive contract compliance review of the Tundra contract (W91B4L-09-D-0024 and Task Order 00081C). DCMA-A provided the contract review results on April 25, 2011, to the Deputy Director, TF SPOTLIGHT.

Based on the results of the review, DCMA-A issued a Level III Corrective Action Request (CAR) to Tundra dated May 7, 2011. Tundra responded to the CAR with a Corrective Action Plan (CAP) on June 15, 2011. After the review of all required documentation, DCMA fully accepted Tundra's CAP and closed the CAR on July 6, 2011. However, the contract continues to be audited by DCMA-A through the support of the Contracting Officer Representatives and the DCMA-A Quality Assurance Representatives. Additionally, DCMA-A has documented

Tundra's unsatisfactory performance at FOB Frontenac in the Joint Contingency Contracting System for SCO-A's use in evaluating contractor performance.

Follow-on to AR 15-6 and Criminal Investigation

The USFOR-A Staff Judge Advocate identified one (1) preliminary inquiry, one (1) AR 15-6 investigation, and one (1) Criminal Investigation Division investigation related to this incident. No Top Secret investigations were identified.

Pre-March 2011 Vetting and Screening Process

In early 2011, ISAF, in coordination with ANSF, implemented the use of the eight-step vetting process to mitigate potential insider threats within the ANSF. The eight-step process is consistent with cultural practices and, to reduce infiltration, enhanced with modern technology. The eight-step process consists of:

1) Valid Tazkera (Afghan identity card);
2) Two letters from village elders or other guarantors;
3) Personal information, including name, father's name, village, and two photos;
4) Criminal records check through MoI, supplemented with an Army G2-record check by Ministry of Defense;
5) Application with validation stamp from recruiting authority;
6) Drug screening;
7) Medical screening; and
8) Biometric collection.

The biometric collection was initiated for all ANSF recruits in September 2009, and once collected the data is downloaded into the Afghan Automated Biometric Identification System (ABIS) to vet against all criminal records.

The ANSF vetting process is also supported by information sharing. ISAF and ANSF biometrics data is shared to help identify potential threats. Coalition mentors also provide oversight to the vetting process. The eight-step process is applied to new ANSF recruits at point of entry. As a result of the comprehensive vetting process, ANSF typically denies approximately 12% of all recruits entry into the ANSF every month.

Before March 2011, PSC guards were not subject to the ANSF eight-step vetting process. Instead, prior to receiving arming authorization, PSC personnel biometric data was verified and

validated by TF SPOTLIGHT. Upon receipt of monthly arming rosters from contract agencies or arming requests from requiring activity commanders (RACs), TF SPOTLIGHT would verify that each PSC guard had been biometrically enrolled using the guard's Tazkera number, which is an identifier similar to a U.S. Social Security number. TF SPOTLIGHT verifications also searched for evidence of past misconduct that may have been uploaded in the biometric-enabled watch list in the ABIS, which can compare a guard's biometrically-enrolled information against stored biometric data, such as latent fingerprints recovered from IEDs, to flag potential bad actors.

If the guard was found in the database and not on a watch list, he was then checked as "verified" in the TF SPOTLIGHT database and validated. If validated, the guard's arming authorization packet was moved forward. If not verified, the packet was rejected and returned to the PSC.

Training

Well before the incident at FOB Frontenac in March 2011, all commanders were directed to train their units on tasks to maintain base camp defense/security, establish security, react to contact, conduct antiterrorism awareness training, maintain situational awareness, and conduct pre-combat checks or inspections for each mission. The Army publishes these requirements in pre-deployment training guidance, which is updated approximately every 6 months and is prescribed for every unit and Soldier deploying. Clearly, infiltration of friendly forces is recognized during training as one of the many hybrid threats – with contracted security forces being only one variable – in our current and future operational environments associated with counterinsurgency missions.

The OEF Lessons Learned Forum, co-chaired by the Army G-3/5/7 and the Commanding General of TRADOC Combined Arms Center, accepted "inside-the-wire threats" in partnering environments as one of the major areas to review. To date, outcomes of the review include increasing integration of insider threats into scenarios at our Combat Training Centers, as well as a dedicated push to publish and make available on-line the Center for Army Lessons Learned Handbook, titled "Inside the Wire Threat-Afghanistan." Army anticipates a publication date on or about March 2012, pending approval by the ISAF Commander.

The Army believes that the current pre-deployment training emphasis adequately prepares Soldiers to detect and protect against inside-the-wire attacks, and the Army will continue to emphasize insider threats. Deploying and deployed organizations must continue their current close coordination in preparation for assuming missions, with a special topic of discussion on the changes concerning the screening, vetting, and employment of PSCs in Afghanistan.

Post-March 2011 Vetting and Screening

PSC Vetting Procedures. Following the insider attack at FOB Frontenac, USFOR-A reviewed their procedures regarding local national contractors and PSC guard personnel. In April 2011, USFOR-A published FRAGO 11-086 directing U.S. Forces to conduct an internal security review of bases and increase force protection measures. Specifically, FRAGO 11-086 directed commanders to review current intelligence and visibly implement appropriate force protection measures immediately, both inside and outside installations, in order to mitigate the threat of unauthorized access, personnel-borne improvised explosive devices (PBIEDs), and complex attacks.

In May 2011, USFOR-A published a modification to FRAGO 11-086. The modification directed commanders to implement procedures to conduct random checks for PSC readiness, discipline, equipment, uniforms, and break-living areas, to ensure all PSC personnel are badged and biometrically enrolled. The modification also directed commanders to conduct weekly biometric screening of local nationals against updated watch lists.

In June 2011, USFOR-A published FRAGO 11-128, Policy for Arming DoD Contractors and Civilians operating in the Combined Joint Operations Area - Afghanistan. The FRAGO directed contracting agencies and RACs to ensure that all DoD contractors are biometrically enrolled and screened prior to receiving a badge or being allowed to carry a weapon. Contracting agencies and RACs were directed to ensure that biometric information is updated and that contractors are barred from installations if they are released from PSC employment for any reason that may affect the security of U.S. or coalition personnel.

Afghan Public Protection Force (APPF) Vetting Procedures. In August 2010, President Karzai decreed that all PSCs would be disbanded by March 2012. In order to provide PSC services GIRoA established the APPF as a state-owned enterprise. ISAF received a waiver to use PSCs through March 2013 as APPF comes on line.

APPF was placed under the administrative control of MoI. MoI will oversee the administrative functions, training, and standardization of all risk management consultants (RMC) and security personnel. ISAF is providing mentor support to APPF headquarters to help establish effective systems and provide oversight. This includes oversight of APPF screening and vetting procedures.

Part of the standardization of APPF is the implementation of a screening process similar to ANSF's eight-step process. The APPF vetting process includes the following:

1) Valid Tazkera (Afghan identity card);

2) Two letters from elders and/or guarantors;
3) Personal information;
4) Criminal records check;
5) Drug screening;
6) Medical screening; and
7) Biometric collection and enrollment in MoI's system for check against watch lists.

The recruiting packet verification is the only step from ANSF's eight-step process not included in the APPF system. As most PSCs already use a process similar to the one described above, the only new requirements are the drug test and biometric enrollments in the Afghan system. PSCs previously only enrolled biometric data in DoD systems

U.S. advisors are aligned against the personnel department of APPF and will monitor compliance and effectiveness of the screening process. Biometric verifications will continue on the DoD system as they do now. U.S. forces will still enforce the guidance in FRAGOs 11-086 and 11-128 once PSCs are disbanded and APPF is fully established.

Special Operation Forces (SOF) currently employs approximately 2600 Afghan Security Group (ASG) forces under PSC contracts at a value of approximately $40M per year. At present, no SOF units employ APPF personnel, but there is a plan to transition to APPF services in 2013 to comply with President Karzai's Presidential decree.

Use of Afghan Nationals to Provide Security to U.S. Bases

To enable the transition from PSCs to APPF, ISAF has set up an APPF Advisory Group (AAG) to work closely with GIRoA to build and shape APPF. APPF currently counts approximately 1400 personnel in the force and are looking to grow to approximately 25,000 by March 2013. All APPF personnel will be vetted using the seven-step process, and any current PSCs who have not been vetted with this process, will be re-vetted.

Currently, AAG is working with MoI to increase their capability, with the initial goal of developing the capacity to provide services by March 2012, and provide full security with ISAF oversight by March 2013. MoI is on-track to implement this goal and provide vetting of all personnel as they grow the force through March 2013.

As APPF numbers and capabilities grow, those forces will gradually move to take the lead in security, especially as U.S. forces draw-down. Given ISAF's waiver to use PSCs through March 2013, DoD will have ample time to ensure that GIRoA, specifically MoI, has

appropriately implemented and can maintain the stringent vetting and screening processes we have worked to standardize throughout APPF.

Notification Timeline

The Department of the Army provides a deceased member's next of kin, via Service casualty assistance officers, copies of all requested reports as soon as they are available. Typically, these include reports of administrative investigations (e.g., an AR 15-6 investigation), autopsy reports, and Criminal Investigation Division (CID) reports. Casualty reports provided to next of kin are redacted consistent with the non-disclosure provisions of the Freedom of Information Act. It is the Department's practice not to provide such casualty investigations to Congress prior to disclosing the findings to the family of the decedent.

In this case, the AR 15-6 investigation into the attack at FOB Frontenac was approved by the RC-S commanding general on May 7, 2011. Due to a significant backlog in the redaction of investigations in theater, the casualty assistance officer did not receive the redacted AR 15-6 report until October 17, 2011. The delivery of the report was delayed at the request of the family of one of the deceased Soldiers. The casualty assistance officer delivered the report to the family on December 20, 2011.

The CID investigation was closed on November 11, 2011. After redactions were completed, the report of investigation was mailed to the families' casualty assistance officers on January 11, 2012, and we are awaiting confirmation of delivery to one of the families.

We hope these answers have provided you greater clarity on the measures the Department has taken – and is taking – to guard our troops against green-on-blue attacks. In contingency environments like Afghanistan, we can mitigate risk, but we can't fully eliminate it. We are confident, though, that the vetting procedures we have implemented offer the best opportunity to both identify those individuals who could pose insider threats and bar those individuals from serving as security personnel.

Thank you for the work you do on behalf of our servicemen and women, as well as your concerted efforts to ensure their protection and safety as they complete their mission in Afghanistan. We stand ready to answer questions from the Committee.

WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING

FEBRUARY 1, 2012

RESPONSE TO QUESTION SUBMITTED BY MR. CONAWAY

General TOWNSEND. DOD has established a set of counterinsurgency training and operational standards to focus U.S. military units on specific requirements prior to and during their deployments to Afghanistan. Some of the skills are not Afghanistan-specific, such as "understand the operational environment" while others apply directly to current operations such as "establish combat outpost." A specific requirement relative to enhancing force protection aboard U.S. forward operating bases is conducting a "relief in place" during unit turnovers. This task involves incoming/outgoing commanders reviewing all current security conditions and sharing relevant force protection information including standard operating procedures. This information sharing also includes reviewing the status of local Afghans or Afghan National Security Force personnel living and/or working aboard the base. [See page 21.]

RESPONSE TO QUESTION SUBMITTED BY MR. JOHNSON

General TOWNSEND. Part of the standardization of APPF is implementation of a screening process similar to ANSF's eight-step process. The APPF vetting process includes the following:

1) Valid Tazkera (Afghan identity card); 2) Two letters from elders and/or guarantors; 3) Personal information; 4) Criminal records check; 5) Drug screening; 6) Medical screening; and 7) Biometric collection and enrollment in MoI's system for check against watch lists.

The recruiting packet verification is the only step from ANSF's eight-step process not included in the APPF system. As we begin to transition to APPF in the next few months we will be able to assess the adequacy and effectiveness of this vetting process in relation to recruitment and employment of APPF. The vetting process has been effective and adequate to screen ANSF and we have already turned away several APPF recruits using the seven-step process. A most recent example occurred within an APPF training class where 21 recruits were screened out due to vetting issues and drug screening failures. [See page 24.]

RESPONSE TO QUESTION SUBMITTED BY MR. SCOTT

Mr. SEDNEY. We do not specifically track this information. Afghanistan is a country in which the majority of the population is illiterate. More than 80 percent of all Afghan National Security Forces (ANSF) recruits are illiterate when they enter the service. Less than 30 percent of the ANSF are literate to the international literacy standard. We have seen high-profile events such as the attack at Kabul International Airport conducted by educated Afghan officers. However, we have not directly studied whether literacy and education are correlated to the likelihood of attack. [See page 25.]

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

FEBRUARY 1, 2012

QUESTIONS SUBMITTED BY MR. MCKEON

Mr. MCKEON. What department or agency was responsible for issuing the contract to Tundra and making sure it did what it promised to do in providing security for the base?

Mr. MOTSEK. The Senior Contracting Official—Afghanistan (SCO–A) of the Joint Theater Support Contracting Command let the contract. The Defense Contract Management Agency—Afghanistan (DCMA–A) was responsible for the management of the contract (W91B4L–09–D–0024 and Task Order 00081C).

Mr. MCKEON. It looked like Tundra (a Canadian company) may have had an Afghan subsidiary involved in paying the Afghan personnel. If the local hires were not directly employed by the Canadian company (Tundra) that received the contract from the U.S. Government (and paid for by our tax dollars), is the private contractor still required to be responsible for control and compliance with our rules of the security personnel on the ground (including the Afghan employee of Tundra that attacked our son and his fellow soldiers)?

Mr. MOTSEK. Contract W91B4L–09–D–0024 was awarded to Tundra Security Consultants Afghanistan (Tundra SCA), which is the Afghan-owned subsidiary of Tundra Strategies of Canada. Although Afghan-owned and operating with a mostly Afghan staff, Tundra SCA operates with a Canadian management team. The contract was not awarded to Tundra Strategies of Canada, and Tundra SCA's personnel were not hired by that company. Under the terms of the contract, Tundra SCA was responsible for control of security personnel on the ground and compliance with our rules and regulations, pursuant to the terms of its contract.

Mr. MCKEON. Are these private security contractors like Tundra providing security at the base also allowed to participate in combat operations with our troops?

Mr. MOTSEK. No. Private Security Company (PSC) contractors are restricted from performing combat functions per Department of Defense Instructions (DODI) 1100.22, 3020.50, and 3020.41, the Defense Federal Acquisition Regulations (DFARs), and the terms of their contracts. Use of force by PSC personnel is limited to self-defense, the defense of others, and the preservation of designated critical or inherently dangerous property against unlawful attack.

Mr. MCKEON. What actions were taken against the private security contractor for any failure to follow required procedures for vetting and supervision of their personnel?

Mr. MOTSEK. Tundra SCA's official records did not indicate that the perpetrator of the Forward Operating Base (FOB) Frontenac attack was previously terminated because he posed a threat, as the allegation was investigated and determined to be unsubstantiated. He had been biometrically enrolled during his previous term of employment with Tundra SCA, but had not yet been re-enrolled at the time of the incident, although a request for re-enrollment had been submitted.

Based on the results of the review, DCMA–A issued a Level III Corrective Action Request (CAR) to Tundra SCA dated May 7, 2011. Tundra SCA responded to the CAR with a Corrective Action Plan (CAP) on June 15, 2011. After the review of all required documentation, DCMA–A fully accepted Tundra SCA's CAP and closed the CAR on July 6, 2011. However, the contract continues to be audited by DCMA–A through the support of the Contracting Officer Representatives and the DCMA–A Quality Assurance Representatives. Additionally, DCMA–A has documented Tundra SCA's unsatisfactory performance at FOB Frontenac in the Joint Contingency Contracting System for SCO–A's use in evaluating contractor performance.

Mr. MCKEON. What vetting was the private contractor (Tundra) required to perform before entrusting its guard with a weapon around our troops?

Mr. MOTSEK. At the time of the FOB Frontenac incident, Tundra SCA was contracted to provide security at nine (9) installations in Afghanistan. Pursuant to the terms of its contract, Tundra SCA was required to submit a plan detailing its processes for hiring employees, performing background checks, and providing the results of the background check to the contracting officer for review and acceptance.

The plan submitted by Tundra SCA required agency checks at both the local and national level. Local agency checks included identity verification via valid Tazkera (the Afghan identity card), verification of work history, address confirmation,

fingerprinting, and a local police check to receive a clearance certificate for each employee. National agency checks required the contractors to submit a completed employee information package to the Afghanistan Ministry of Interior (MoI) and the Afghanistan National Directorate of Security (NDS), which investigates major crime and potential connections to terrorist organizations. Pending a successfully cleared background check, the Afghanistan Ministry of Foreign Affairs would then issue a certificate of successful vetting and acceptance.

Additionally, Tundra SCA was required to support the Government of the Islamic Republic of Afghanistan (GIRoA) portion of the vetting process by submitting requests for biometric enrollment, ensuring the availability of language interpretation services during the screening and enrollment processes, and requesting Global Unique Identification numbers from GIRoA enrollers to verify each individual enrollment. The action with GIRoA was accomplished; the re-enrollment with the U.S. Government biometric database was pending. The individual was still in the U.S. database due to his previous employment.

Prior to submission of an arming request, all local nationals and third-country nationals must submit to full biometric enrollment. Additional routine biometric screening then continues in accordance with local installation policies and procedures. Like all contractors, Tundra SCA is required to notify the contracting officer's representative, the local installation Force Protection agency, and the theater arming approval authority immediately if individuals are revealed as potential security risks during biometric processing.

Tundra SCA was also required to develop a process by which employee termination would be communicated to the contracting officer and local installation Force Protection agencies. The aim is to prevent unauthorized access, and to communicate potential security risks concerning individuals terminated for cause to NDS for biometric watch list consideration. To prevent the rehiring of high-risk personnel, all contractors were additionally required to develop a plan of action to address the tracking and communication of employee dismissals to all sites managed by the contractor. Finally, according to the terms of its contract, Tundra SCA was required to maintain records on the screening status of its employees for six months following termination.

Mr. MCKEON. What can and needs to be done to insure that our troops are only guarded by fellow U.S. troops while on base in areas that we are conducting military actions such as Afghanistan?

Mr. SEDNEY. The contractors' ability to provide specific security functions frees up U.S. Forces to conduct more combat-focused missions. Contractors perform their missions well and provide essential support for the conduct of operations in Afghanistan as they do worldwide. Without contractors (20,000 presently performing the function today), we would have to divert forces from essential combat tasks to perform these security functions. The use of civilians to guard U.S. bases in Afghanistan, based upon threat analysis, is consistent with our use of them elsewhere in the world and in previous conflicts.

QUESTIONS SUBMITTED BY MR. KISSELL

Mr. KISSELL. Are there any other related, recorded problems on this issue than those that led to a death?

General DAHL. The investigation conducted by Regional Command-South identified a number of shortcomings in the policies governing the hiring and management of Afghan private security contractors and the execution of those policies. These problems are discussed in some detail in the investigation report, a copy of which was provided to the Committee before the hearing. Although the investigation found that those specific issues did not lead directly to the deaths of the Soldiers at FOB Frontenac, the command took immediate steps to correct the problems to provide an additional measure of security for our Soldiers.

Mr. KISSELL. Are there other companies with similar security responsibilities as Tundra Strategies, which are setting good examples, such that U.S. forces would want to see emulated? Furthermore, how closely are U.S. forces monitoring these companies to ensure that there aren't other up-and-coming potential assailants?

General DAHL. I defer to the Joint Staff and OSD regarding current policies and the performance of private security contractors (PSCs) in theater. The policies in place at the time of the FOB Frontenac attack and the subsequent improvements implemented within Regional Command-South applied to all private security contractors, to include to requirement to screen PSC employees and to mitigate the risks associated with insider threats.

Mr. KISSELL. Once Afghan nationals are hired to provide security to U.S. Forces, how much access are they allowed throughout the forward operating base or military facility? Similarly, why aren't there 10% random daily biometric checks for Afghan nationals accessing a U.S. facility with the purpose of providing security?

General DAHL. I defer to the Joint Staff and OSD on current theater policies regarding access by private security contractors (PSCs). During the time I was deployed to Regional Command-South, access was based on contact performance requirements, with oversight provided by the local commander and contracting officer representative. Likewise, specific force protection measures were applied by local commanders consistent with theater policies and their own risk assessments. As noted in the materials provided to the Committee before the hearing, the Regional Command-South commander directed that all subordinate Task Forces conduct random, 50 percent monthly screening/verification of all PSC employees to ensure they were not on the Afghan Watch List.

Mr. KISSELL. Are there any other related, recorded problems on this issue than those that led to a death?

General TOWNSEND. Since May 2007, ISAF elements identified 42 ANSF and 3 PSC related insider incidents. The cause of each event varies. We utilize the lessons learned in each attack to identify potential counter-measures and reduce the primary causes of insider attacks.

Mr. KISSELL. Are there other companies with similar security responsibilities as Tundra Strategies, which are setting good examples, such that U.S. forces would want to see emulated? Furthermore, how closely are U.S. forces monitoring these companies to ensure that there aren't other up-and-coming potential assailants?

General TOWNSEND. USFOR–A FRAGO 11–128 sets specific standards for all of the private security companies supporting U.S. installations. As with all contracts, contractor's performance is monitored against stated contract requirements and standards. Terms and conditions of the contract provide a means to ensure that the contractor is effectively performing, e.g., penalties, show cause (notice of non-performance), and termination. The IJC Armed Contractor Oversight Directorate (ACOD) monitors all of the PSCs in order to enforce compliance with US requirements. Each unit and installation commander is also responsible for monitoring and ensuring compliance by all PSC personnel in order to reduce the future insider threat.

Mr. KISSELL. Once Afghan nationals are hired to provide security to U.S. Forces, how much access are they allowed throughout the forward operating base or military facility? Similarly, why aren't there 10% random daily biometric checks for Afghan nationals accessing a U.S. facility with the purpose of providing security?

General TOWNSEND. The level of access provided to U.S. Military facilities is based on the specific contract. USFOR–A FRAGOs 11–128 and 11–086 set specific requirements for units using contract security personnel. Contractors are required to wear access badges issued via biometric registration in order to ensure that they operate in areas authorized by their contract.

USFOR–A FRAGO 11–086 now directs commanders to conduct weekly biometric screening of local national contractors. Commanders may use their discretion in determining how to execute the required weekly screening. The use of a 10% random check would be up to the discretion of the requiring activity commander.

Mr. KISSELL. Are there any other related, recorded problems on this issue than those that led to a death?

Mr. MOTSEK. Since May 2007, ISAF elements identified 42 ANSF and 3 PSC related insider incidents. The cause of each event varies. We utilize the lessons learned in each attack to identify potential counter-measures and reduce the primary causes of insider attacks.

Mr. KISSELL. Are there other companies with similar security responsibilities as Tundra Strategies, which are setting good examples, such that U.S. forces would want to see emulated? Furthermore, how closely are U.S. forces monitoring these companies to ensure that there aren't other up-and-coming potential assailants?

Mr. MOTSEK. USFOR–A FRAGO 11–128 sets specific standards for all of the private security companies supporting U.S. installations. As with all contracts, contractor's performance is monitored against stated contract requirements and standards. Terms and conditions of the contract provide a means to ensure that the contractor is effectively performing, e.g., penalties, show cause (notice of non-performance), and termination. The IJC Armed Contractor Oversight Directorate (ACOD) monitors all of the PSCs in order to enforce compliance with US requirements. Each unit and installation commander is also responsible for monitoring and ensuring compliance by all PSC personnel in order to reduce the future insider threat.

Mr. KISSELL. Once Afghan nationals are hired to provide security to U.S. Forces, how much access are they allowed throughout the forward operating base or military facility? Similarly, why aren't there 10% random daily biometric checks for Afghan nationals accessing a U.S. facility with the purpose of providing security?

Mr. MOTSEK. The level of access provided to U.S. Military facilities is based on the specific contract. USFOR–A FRAGOs 11–128 and 11–086 set specific requirements for units using contract security personnel. Contractors are required to wear access badges issued via biometric registration in order to ensure that they operate in areas authorized by their contract.

USFOR–A FRAGO 11–086 now directs commanders to conduct weekly biometric screening of local national contractors. Commanders may use their discretion in determining how to execute the required weekly screening. The use of a 10 percent random check would be up to the discretion of the requiring activity commander.

Mr. KISSELL. Are there any other related, recorded problems on this issue than those that led to a death?

Mr. SEDNEY. Since May 2007, International Security Assistance Force (ISAF) elements have identified 42 Afghan National Security Forces (ANSF) and 3 Private Security Contractor (PSC)-related insider incidents. The facts of each event are different. We utilize the lessons learned from such incidents to identify potential counter-measures and reduce the primary causes of insider attacks.

Mr. KISSELL. Are there other companies with similar security responsibilities as Tundra Strategies, which are setting good examples, such that U.S. forces would want to see emulated? Furthermore, how closely are U.S. forces monitoring these companies to ensure that there aren't other up-and-coming potential assailants?

Mr. SEDNEY. USFOR–A Fragmentary Order 11–128 sets specific standards for all of the private security contractor (PSCs) supporting U.S. installations. As with all DoD contracts, the contractor's performance is monitored against stated contract requirements and standards. The terms and conditions of the contract provide a means to ensure that the contractor is effectively performing, e.g., penalties, show cause (notice of non-performance), and termination. The U.S. Forces-Afghanistan Armed Contractor Oversight Directorate (ACOD) monitors all U.S. PSCs in order to enforce compliance with U.S. requirements. Each unit and installation commander is also responsible for monitoring and ensuring compliance by all PSC personnel in order to reduce the future insider threat.

Mr. KISSELL. Once Afghan nationals are hired to provide security to U.S. Forces, how much access are they allowed throughout the forward operating base or military facility? Similarly, why aren't there 10% random daily biometric checks for Afghan nationals accessing a U.S. facility with the purpose of providing security?

Mr. SEDNEY. The level of access provided to U.S. military facilities is based on the specific contract. USFOR–A Fragmentary Orders (FRAGOs) 11–128 and 11–086 set specific requirements for units using contract security personnel. Contractors are required to wear access badges issued via biometric registration in order to ensure that they operate in areas authorized by their contract.

USFOR–A FRAGO 11–086 now directs commanders to conduct weekly biometric screening of local national contractors. Commanders may use their discretion in determining how to conduct the required weekly screening. The use of a 10 percent random check would be up to the discretion of the requiring activity commander.

QUESTIONS SUBMITTED BY MR. RUPPERSBERGER

Mr. RUPPERSBERGER. A background investigation for U.S. personnel can range from a simple criminal records check to a more thorough review, like what is done for many in the Intelligence Community. When hiring Afghan Nationals to protect the personal security of U.S. forces and/or assets, it makes sense that background investigations should be done for them as well. However, it does not seem possible to do the same level of background investigation in Afghanistan as those done in the United States. Are some types of background investigation applied to Afghan Nationals, and how do you plan on incorporating those results into your employment decision?

General TOWNSEND. Agency checks at both local and national level are required. Local agency checks include identity verification via valid Tazkera (the Afghan identity card), verification of work history, address confirmation, fingerprinting, and local police check to receive a clearance certificate for each employee. National agency checks require contractors to submit a completed employee information package to the Afghanistan Ministry of Interior (MoI) and the Afghanistan National Directorate of Security (NDS), which investigates major crime and potential connections to terrorist organizations. Pending a successfully cleared background check, the Af-

ghanistan Ministry of Foreign Affairs would then issue a certificate of successful vetting and acceptance.

Additionally, contractors are required to support the Afghan Government (GIRoA) portion of the vetting process by submitting requests for biometric enrollment, ensuring availability of language interpretation services during the screening and enrollment processes, and requesting Global Unique Identification number from GIRoA enrollers to verify each individual enrollment.

Prior to submission of an arming request, all local nationals and third-country nationals must submit to full biometric enrollment. Additional routine biometric screening then continues in accordance with local installation policies and procedures. All contractors are required to immediately notify the contracting officer's representative, the local installation Force Protection agency, and the theater arming approval authority of individuals who are revealed as potential security risks during biometric processing.

Contractors are also required to develop a process by which employee termination would be communicated to the contracting officer and local installation Force Protection agencies. While the aim is to prevent unauthorized access, the process also communicates potential security risks to NDS for biometric watch list consideration. To prevent the rehiring of high-risk personnel, all contractors are additionally required to develop a plan of action to address the tracking and communication of employee dismissals to all sites managed by the contractor. Finally, according to the terms of its contract, contractors are required to maintain records on the screening status of its employees for six months following termination.

Mr. RUPPERSBERGER. A background investigation for U.S. personnel can range from a simple criminal records check to a more thorough review, like what is done for many in the Intelligence Community. When hiring Afghan Nationals to protect the personal security of U.S. forces and/or assets, it makes sense that background investigations should be done for them as well. However, it does not seem possible to do the same level of background investigation in Afghanistan as those done in the United States. Are some types of background investigation applied to Afghan Nationals, and how do you plan on incorporating those results into your employment decision?

Mr. MOTSEK. Agency checks at both local and national level are required. Local agency checks include identity verification via valid Tazkera (the Afghan identity card), verification of work history, address confirmation, fingerprinting, and local police check to receive a clearance certificate for each employee. National agency checks require contractors to submit a completed employee information package to the Afghanistan Ministry of Interior (MoI) and the Afghanistan National Directorate of Security (NDS), which investigates major crime and potential connections to terrorist organizations. Pending a successfully cleared background check, the Afghanistan Ministry of Foreign Affairs would then issue a certificate of successful vetting and acceptance.

Additionally, contractors are required to support the Afghan Government (GIRoA) portion of the vetting process by submitting requests for biometric enrollment, ensuring availability of language interpretation services during the screening and enrollment processes, and requesting Global Unique Identification number from GIRoA enrollers to verify each individual enrollment.

Prior to submission of an arming request, all local nationals and third-country nationals must submit to full biometric enrollment. Additional routine biometric screening then continues in accordance with local installation policies and procedures. All contractors are required to immediately notify the contracting officer's representative, the local installation Force Protection agency, and the theater arming approval authority of individuals who are revealed as potential security risks during biometric processing.

Contractors are also required to develop a process by which employee termination would be communicated to the contracting officer and local installation Force Protection agencies. While the aim is to prevent unauthorized access, the process also communicates potential security risks to NDS for biometric watch list consideration. To prevent the rehiring of high-risk personnel, all contractors are additionally required to develop a plan of action to address the tracking and communication of employee dismissals to all sites managed by the contractor. Finally, according to the terms of its contract, contractors are required to maintain records on the screening status of its employees for six months following termination.

○