

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  
10<sup>TH</sup> 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

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 17<sup>th</sup> 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.