Sensitive Material

The Inspector General Department of the Air Force

Report of Inquiry (S9044P)

Joint Base Andrews – Unauthorized Access

(Base & Flight Line Access Incident)

March 2021

DO NOT OPEN COVER WITHOUT A NEED TO KNOW--
PROTECTED COMMUNICATION TO IG

REPORT OF INQUIRY (Case S9044P)

CONCERNING

INCIDENT REVIEW:
JOINT BASE ANDREWS – UNAUTHORIZED ACCESS

PREPARED BY
DAF/IGS
March 2021

I. INTRODUCTION

The Secretary of the Air Force (SAF) directed the Department of the Air Force Inspector General to review the unauthorized access incident that occurred on Joint Base Andrews (JBA) on 4 Feb 21.

II. BACKGROUND & EXCUTIVE SUMMARY

At 0716 on 4 Feb 21, [redacted][1] gained unauthorized access to JBA through the Virginia Gate. [redacted] then proceeded via an unknown route to the Base Exchange (BX). [redacted] entered the BX and was recorded on surveillance cameras walking throughout the food court. After a little over an hour, [redacted] returned to his vehicle and left the BX parking lot. From that point in time, his whereabouts were unknown until personnel at the 89th Airlift Wing (89 AW) passenger terminal witnessed him entering the terminal nearly four hours later. After a brief exchange with the personnel at the terminal, [redacted] left the terminal. [redacted] proceeded to flight line Entry Control Point (ECP) [redacted], where he accessed the flight line through a gap in the outbound lane gate. The gap in the gate was due to a malfunction causing it to not fully close.

After entering the flight line, [redacted] entered the 89 AW Mass Parking Area (MPA) and walked toward a C-40 aircraft parked on Row 6. At the time, the aircraft was postured for aircrew training with air-stairs in place and the main entry door open. Two aircrew members were on board conducting training at the Communications System Operators position. [redacted] proceeded up the stairs and boarded the aircraft. The aircrew members observed him walking toward the back of the aircraft and then again when he exited the aircraft a few minutes later. After exiting the aircraft, [redacted] walked back in the direction of ECP [redacted] and, prior to exiting the restricted area, was engaged by 316th Security Forces Squadron (316 SFS) Defenders. [redacted] was escorted out of the restricted area and arrested for unauthorized access to the flight line.

[1] [redacted] will be referred to as [redacted] for the remainder of the report.

This review found three issues led to [redacted] unauthorized access to JBA and the C-40 aircraft. The first involved human error, as a fully qualified and trained SFS [redacted] serving as a gate guard failed to follow proper procedures and wrongfully allowed [redacted] to access the base. Second, the automatic gate at ECP [redacted] had malfunctioned, allowing unauthorized pedestrian access to the flight line. Third, personnel who first saw [redacted] on the aircraft did not challenge his presence. Fortunately, two astute Air Force members from the passenger terminal, upon recognizing they each had unusual interactions with [redacted], alerted Security Forces. Once Security Forces were notified, they responded, intercepted, and detained [redacted] in less than two minutes.

Immediately after [redacted] was apprehended, JBA leadership quickly acted to ensure installation security. Base entry gate personnel were alerted and refocused on security procedures, ECP [redacted] gate was repaired and secured, and 316 SFS personnel and 89 AW personnel addressed security policy issues regarding the flight line area [redacted] accessed.

At no point was an operational DV aircraft mission or personnel threatened. There is no evidence indicating that [redacted] intended to do harm to any Air Force personnel or equipment. Finally, there is no evidence to indicate [redacted] had any support or assistance in accessing the installation.

III. CHRONOLOGY OF 4 FEB 21 EVENTS

TIME (EST)	EVENT
0716	[redacted] arrived at the Virginia Gate. A 316 SFS gate guard, [redacted], failed to appropriately check identification/credentials for installation access, improperly allowing [redacted] to proceed through the gate and onto base.
0717 - 0810	[redacted] whereabouts unknown. No sign of [redacted] or [redacted] vehicle.
0810	[redacted] vehicle entered the BX parking lot via Arnold Ave.
0821	[redacted] exited his car and walked toward the BX entrance. Video inside shows entering and exiting the BX food court area.
0934	[redacted] returned to his car and drove out of the BX parking lot in direction of Arnold Ave.
0934 - ~1145	[redacted] whereabouts unknown. No sign of [redacted] or [redacted] vehicle.
~1145	[redacted], 89 AW Passenger Terminal [redacted], observed [redacted] entering the passenger terminal. [redacted] said [redacted] looked out the glass doors toward the flight line, then walked toward the VIP lounge door. [redacted] interrupted [redacted] and asked, "Can I help you?" [redacted] responded by saying something about needing a ride, then walked back toward the passenger terminal front door. [redacted] followed [redacted] to the door and observed [redacted] standing outside across the street. [redacted] said it looked like [redacted] was waiting for a ride.

~1208	[redacted] walked through a gap in the [redacted] gate at ECP [redacted] and gained access to the flight line.
~1210	While driving back to the passenger terminal after doing vehicle checks, [redacted] 89th Aerial Port Squadron, observed [redacted] walking on the flight line in the direction of Row 6.
1212	Tower camera video showed [redacted] crossing the red line and walking toward the C-40 aircraft parked on Row 6.
~1219	[redacted] observed on the aircraft by [redacted], 1 AS, Communication System Operator, and [redacted]. [redacted] was training [redacted] on the aircraft communication systems. They said [redacted] entered the aircraft, walked toward the back of the aircraft, then a few minutes later walked back to the front and exited the aircraft. They did not communicate with [redacted] and did not notify anyone about [redacted] presence on the aircraft.
~1220	[redacted] got back to the passenger terminal and talked to [redacted] She mentioned seeing [redacted] to [redacted], and the two compared what they saw. After talking for a few minutes, [redacted] decided to contact the Base Defense Operation Center (BDOC).
1232	[redacted] contacted the BDOC and mentioned that a potential unauthorized person was on the flight line. The BDOC notified Security Forces and started maneuvering the tower camera to search for [redacted] on the flight line.
1233	Video footage shows [redacted] walking away from the C-40 aircraft toward the ECP [redacted] and a Security Forces truck responding to intercept him.
1233-1234	Security Forces personnel escorted [redacted] outside the red line, and detained him.
1237	Security Forces placed [redacted] into custody.
1239	[redacted] was transported for questioning.
~1300	316 SFS initiated K-9 and Technical Surveillance Counter Measures sweeps of the aircraft and surrounding area.
1314	Air Force Office of Special Investigations (AFOSI) received notification from 316 SFS that [redacted] was in their custody for unauthorized access to the installation and flight line. When searched, [redacted] had a [redacted] ID card, set to expire in [redacted] a [redacted], set to expire in [redacted]; a [redacted] that was set to expire on [redacted] Note: [redacted] were not sufficient documentation to allow access to JBA.
1457	Passenger terminal personnel notified BDOC that the [redacted] gate at ECP [redacted] was stuck open approximately 12 to 18 inches. BDOC notified the 316 personnel who handle FLECS ECP maintenance, who reset the gate then chain-closed the outbound section of ECP [redacted].
1530	K-9 units initiated sweeps of the area around ECP [redacted] and identified the [redacted] vehicle parked in the 89 AW/CC's spot at the passenger terminal.

2100	[redacted] booked under 18 U.S. Code 1382, issued a DD Form 1805 citation, and transferred to Prince George's County Police Department, MD, for having [redacted]

IV. ANALYSIS

AFOSI conducted the following Law Enforcement Checks on 4 Feb 21 for [redacted]:

- A review of the National Criminal Information Center (NCIC) disclosed [redacted] had an extensive arrest history, including more than [redacted] The review also indicated he had an active warrant for his arrest, issued by the [redacted].
- A review of the DoD Law Enforcement Data Exchange (D-DEX) disclosed [redacted] had an [redacted] and an [redacted] from [redacted].
- A review of FBI and Joint Terrorism Task Force Databases disclosed no records on file.
- According to [redacted] was currently unemployed, homeless, and often lived out of [redacted] car.

The DAF/IG review team analyzed the events on 4 Feb 21 in three sections: Base Access, Flight Line Access, and Aircraft Access.

BASE ACCESS

At 0716 on 4 Feb 21, [redacted] drove his car to the Virginia gate, where a 316 SFS gate guard, [redacted], allowed him entry to the base even though [redacted] did not have any Department of Defense affiliation or clearance. At the time, [redacted] was carrying a current [redacted]. While all of his forms of ID were current, none were credentials that authorized [redacted] access to the base.

At the time of the incident, JBA Security Forces were accomplishing "windows up" gate checks due to COVID 19 concerns. The standard operating procedures (SOPs) for these checks fall into three categories:

- Defense Biometric Identification System (DBIDS) capable credentials (IDs): Gate checks of DBIDS capable credentials were accomplished using the DBIDS scanner through the driver's window or the windscreen if the scanner would not pick up through

the driver's window. If the scanner still would not pick up, the gate guard had to ask the driver to lower the window and the guard would physically handle the ID to scan the ID. Once scanned, the DBIDS scanner would indicate green if the individual should be allowed on or red if there was an issue with the ID that would not allow the individual access to the base.

- Other Acceptable Access Credentials: If an individual had authorized credentials that were not DBIDS capable, for example AFOSI or FBI or local police credentials, the gate guard was responsible for recognizing the appropriate credentials and confirming the identity of the individual prior to allowing entry.

- Entry Access List (EAL): If the individual was requesting access based on prior coordination through the EAL, the gate guard would have to verify the identity of the individual by matching the individual's ID to the approved ID shown on the EAL. If the information on the individual's ID did not match the ID information on the EAL, the individual would not be allowed through the gate.

[redacted] did not have a DBIDS ID or other acceptable access credentials and was not on the EAL; thus, he should not have been allowed through the gate and onto JBA.

When shown the 04 Feb 21 video footage of [redacted] at the Virginia Gate, [redacted] acknowledged he was the gate guard in the video who allowed [redacted] vehicle to enter the base. Even after viewing the video, [redacted] could not remember if [redacted] presented his driver's license or any other form of ID prior to driving through the gate. From the video, it is not clear if [redacted] showed any form of ID prior to passing through the gate. It is clear in the video that [redacted] did not actively use his DBIDS scanner and did not check the EAL prior to allowing [redacted] access to the base. When questioned, [redacted] said he got complacent and did not follow the normal procedures when he allowed [redacted] vehicle to pass through the gate.

[redacted] was initially uncooperative and could not, or would not, provide any additional details regarding what happened at the gate. Specifically on 4 Feb 21, he said could not remember which gate he went through and what he did to gain access to the base. [redacted] was confused and his statements were disjointed, but there was no indication that [redacted] was under the influence of drugs or alcohol. In a later interview conducted on 9 Feb 21, [redacted] was more evasive. This time he said he did not remember anything about being on base and claimed he was under the influence on 4 Feb 21, although he could not, or would not, clarify if he was under the influence of drugs or alcohol or both.

The review team considered the possibility that [redacted] knew [redacted] and knowingly allowed [redacted] access to the base. There is no evidence that indicates [redacted] knew and intentionally allowed [redacted] on base. When questioned, [redacted] said that he did not know [redacted]. While [redacted] was not cooperative and hard to follow during

questioning, he repeatedly stated he did not know or meet anyone on base. The gate video does not indicate that [redacted] communicated with or recognized [redacted] when he pulled up to the gate. Finally, the available video and testimonial evidence does not indicate [redacted] met or interacted with anyone on base other than his brief conversation with [redacted] in the passenger terminal.

According to 316 SFS leadership, [redacted] came on duty at [redacted] on 4 Feb 21 and started an [redacted]. During eight-hour shifts, guards are given a break every two hours. The video shows steady traffic through the gate at 0716, but nothing out of the ordinary as far as crowding. Given it was the [redacted] of his shift, and the reasonable relief cycle employed by the 316 SFS, fatigue should not have been a factor. [redacted] mentioned he was dealing with some personal issues but appeared to be handling things well. He was fully qualified for gate duty and did not have any record of sub-standard performance. This review found no indication that [redacted] should not have been on gate guard duty on 4 Feb 21. Furthermore, during questioning [redacted] did not mention fatigue or ops tempo as contributing factors.

JBA has unique challenges when it comes to other acceptable authorized credentials for accessing the base. There are more than 50 specific credentials with numerous "exceptions" listed in local policy. Although the number of credentials could add to gate guard fatigue, confusion, or frustration, there is no indication other authorized credentials played a role in [redacted] gaining access to the base on 4 Feb 21. [redacted] did not mention other authorized credentials as a contributing factor.

Ultimately, the evidence indicates human error led to [redacted] access to JBA. Based on his statement, [redacted] knew what was required but got complacent and did not follow proper procedures when he allowed [redacted] through the gate.

Note: When the unauthorized access was discovered and [redacted] was detained, the installation commander immediately limited the Trusted Traveler program and changed to a "windows down ID checks" at all entry gates. Furthermore, on 15 Feb 21, the installation commander fully suspended the Trusted Traveler program and directed 100% ID check and vetting of all people entering the base. While these were likely prudent measures to harden the perimeter of the base given the circumstances, there is no indication that the Trusted Traveler program or the "windows up" ID check protocol contributed to [redacted] being allowed access to the base on 4 Feb 21.

Once on the base, there was no capability or immediately apparent reason to track [redacted] vehicle. [redacted]

[redacted] The 316th Wing (316 WG) has already programmed funds for camera upgrades, which will begin later this year. While the upgrades will ensure camera coverage on all gate entry lanes, increase the number of operational cameras at flight line ECPs, and improve the quality of the video captured, they will not allow for full base coverage or enable automatic license plate identification.

After [redacted] entered the Virginia Gate at 0716, there is no evidence to indicate where he went until his vehicle appeared on video from the BX parking lot camera. The video shows [redacted] vehicle entered the BX parking lot from Arnold Ave at 0810. The video then shows he exited his vehicle and entered the BX building at 0816. Video from inside the BX shows [redacted] walking toward the food court. Approximately 1 hour and 15 minutes later, the same camera shows [redacted] walking from the food court toward the BX exit. At 0934, the BX parking lot camera captured [redacted] returning to his car and driving out of the BX parking lot toward Arnold Ave. After [redacted] left the BX parking lot, there is no evidence to indicate his whereabouts until [redacted] observed him in the passenger terminal at approximately 1145. [redacted] monitored [redacted] for a few minutes then asked if he needed assistance. [redacted] said something about needing a ride and then started walking toward the passenger terminal exit. At approximately 1200, [redacted] escorted [redacted] to the passenger terminal exit and subsequently observed him standing across the street from the terminal. The next video contact of [redacted] is at 1212, when the air field tower camera picked up [redacted] on the flight line walking toward Row 6 of the 89 AW MPA. The events after [redacted] left the passenger terminal will be covered in the Flight Line Access section of this report.

Although [redacted] location could not be determined for the entire time he was on base, the evidence supports the conclusion that [redacted] was simply wandering around the base and did not enter the base to meet anyone. During questioning, [redacted] said he came on base because he wanted to see airplanes. He said he made a couple of right turns after he got on base, but he could not provide any further details and did not remember passing the golf course or any specific landmarks. If he did drive straight down Virginia Ave. and then turn right at the T intersection of Virginia Ave. and Menoher Drive, this path would have taken him near the passenger terminal and ECP [redacted]. From this location, [redacted] could have seen the C-40 aircraft parked on the main parking ramp. This route also would have placed him near the intersection of Arnold Ave., which leads to the BX parking lot. [redacted] also mentioned sleeping in his car. It is possible that after leaving the BX parking lot, [redacted] drove to the passenger terminal parking lot and stayed in his car until entering the passenger terminal at around 1145; however, there is no evidence to confirm this is actually what happened.

Conclusion:

On 4 Feb 21, human error at a single point of failure allowed an unauthorized civilian with unknown motives to gain access to JBA. In this case a fully qualified and trained Security Forces gate guard was complacent and failed to follow established procedures. Specifically, the guard did not utilize his DBIDS scanner to check the civilian's credentials and failed to properly identify that the civilian did not have proper authorization to enter the base. Had the guard properly followed normal and established procedures, the civilian's vehicle would have been turned around at the gate.

The base entry process and tracking capability at JBA is consistent with procedures and capabilities across AF installations. This process results in the gate guard presenting a single point of failure, if complacency or a mistake occurs. DBIDS scanning is an important tool; however, it is not a comprehensive back-up system. There is no positive step requirement a gate guard must execute to override, or otherwise document, that access was granted outside of DBIDS authorization. Furthermore, there is no automated backup to alert when the system is not used on a vehicle.

An automated vehicle or personnel identification or tracking system—none of which are present at JBA—would not necessarily prevent unauthorized entry. However, these capabilities would allow for the identification of vehicles entering the base by license plate number, and may afford more situational awareness if an identified threat has entered the base, thus enabling Security Forces to respond appropriately. Furthermore, such a system, along with tracking capability, would allow security personnel to quickly identify and recreate the path any unauthorized vehicle traveled while on the base, thus increasing security.

FLIGHT LINE ACCESS

STANDARDS

AFI 31-101:

8.7. [redacted].

8.7.7. [redacted]

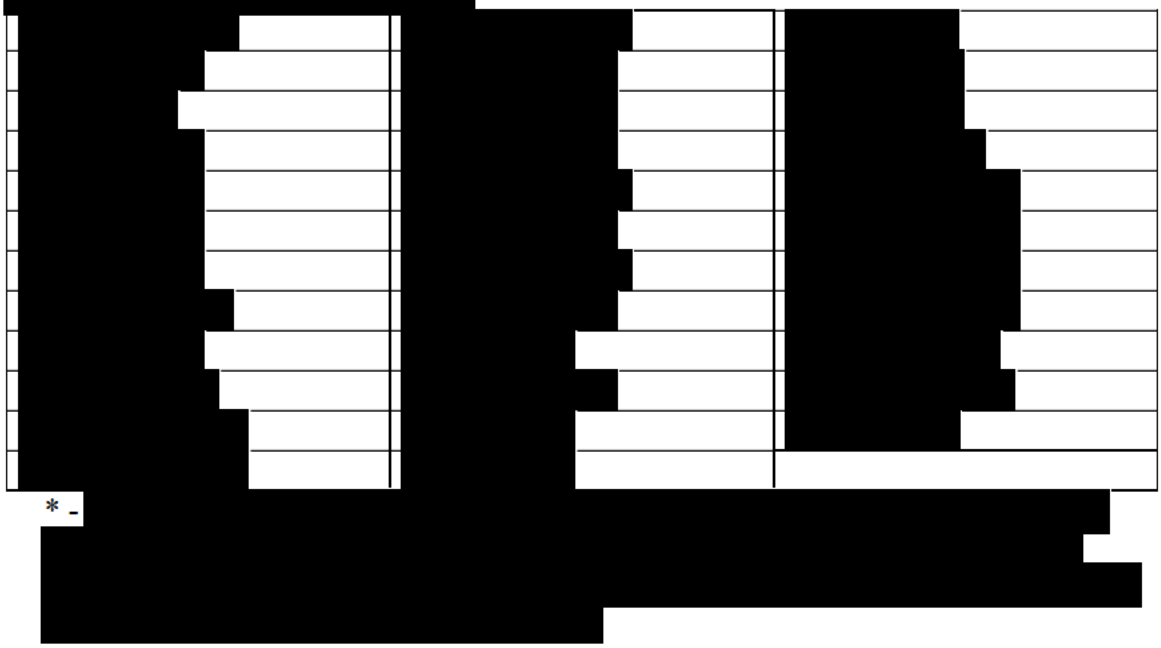
[redacted].

8.2.2.3. [redacted]

[redacted]

8.2.2.3.1. [redacted]

[redacted]



* -

JBAI 31-101:

7.10. [redacted]

7.10.1. [redacted]

Chapter 8 - [redacted]

8.1. [redacted]

8.2.1. [redacted]

8.2.2. [redacted]

8.2.2.4. [redacted]

ANALYSIS OF 4 FEB 21 EVENTS

Evidence shows that JBA ECP [redacted] gate malfunctioned, and on the morning of 4 Feb 21 the exit section of the gate was partially open. At approximately 1210, [redacted] gained access to the flight line through the partially open gate. Once on the flight line, [redacted] proceeded undetected and unchallenged into a restricted area and then onboard an 89 AW aircraft parked on the MPA.

The system failure/malfunction at ECP [redacted] on 4 Feb 21 played a significant role in [redacted] gaining access to the flight line; however, this was not the first time ECP [redacted] had problems. Over the past year, prior to 4 Feb 21, there were six (6) occasions that a malfunction was reported regarding ECP [redacted]. The majority of these malfunctions involved the gate failing to open; however, on 12 Jan 21, the inbound section of ECP stopped one foot short of closing. The 12 Jan 21 malfunction was identified, the limit switch was adjusted, and after the maintenance work, the gate functioned correctly. On 4 Feb 21, after [redacted] was apprehended on the flight line, the outbound section of ECP [redacted] was found stuck partially open. Maintenance technicians responded and reset the local operator box. After the reset, the gate operated correctly, but 316 WG leadership decided to chain the outbound gate closed to preclude any further malfunction and vulnerability.

Local guidance identifies the 316 WG as the "Owner/User" responsible for manning ECP [redacted] when manual operation is required or special events. According to maintenance and the BDOC, 89 AW passenger terminal personnel have done a good job monitoring the gate and coordinating when the gate malfunctions. [redacted]

This section implies that the person actually using the gate at the time is responsible for reporting the malfunction. The instruction then goes on to focus on if the gate fails to open.

The last time the exit section of the ECP [redacted] gate was used was at 1538 on 2 Feb 21. At that time, the user did not identify that the gate was open. The entry section of ECP [redacted] was used by five different users between 2 Feb 21 and 1457[2] on 4 Feb 21. None of those users identified that the exit section of the gate was partially open. There were no visual checks of ECP [redacted] recorded in the blotter between 2 Feb 21 and 4 Feb 21.

According to 316th Security Forces Group (316 SFG) leadership, the area beyond ECP is considered a controlled area rather than a restricted area and section 8.7.7 of AFI 31-101 does not specifically apply. Therefore, there is no specific written guidance or requirement regarding on how often ECP [redacted] has to be checked to ensure it is closed and functioning correctly. Furthermore, there is also no specific OPR identified for checking ECP [redacted] and no requirement to document if or when the gate has been checked.

Further complicating matters at ECP [redacted] is the gate's construction. ECP [redacted] is made up of thick metal vertical slats. The center section of the gate is slightly offset from the moving, entry and exit, sections of the gate. As a result, it is hard to tell visually if the gate is slightly open when looking at the gate from an angle. To clearly see an opening, an observer needs to be positioned perpendicular to the gate and straight out from the center section of the gate.

On the system side, there is no automatic indicator that shows the status of the gate. The gates internal system maintains a log of when the gate was used that can be downloaded, but there is no real-time indication when the gate is in use, if it malfunctions, or the status of the gate. Most importantly, there is no intrusion detection system (IDS) capability at ECP [redacted] or the surrounding flight line fencing. Planned camera upgrades that are scheduled for later this year will result in a camera located outside ECP [redacted], but the upgrades will not add motion sensing or intruder detection.

Once on the flight line, [redacted] was not challenged or detained for not having a restricted area badge while in a controlled area. Per policy guidance, specifically JBAI 31-101, there is an expectation that anyone on the flight line without a visible restricted area badge will be challenged and detained until Security Forces responds. Specifically, the local guidance states, "Every person working within the flight line area is responsible for assisting with airfield protection."

On 4 Feb 21, [redacted] was wearing dark pants, a dark jacket, black high top sneakers, and carrying a brown backpack. On his head, he had a bright red or pink cap that partially covered his ears and had distinctive balls on top that looked a little like mouse ears. Other than the hat, [redacted] outfit resembled the clothing commonly worn by civilian [redacted]

[2] The BDOC was notified that the gate was stuck open at 1457 on 4 Feb 21, see chronology.

[redacted] while on the flight line. According to 89 AW leadership, civilian maintenance personnel from [redacted] characteristically wear dark blue pants and tops with black boots, but in the winter the outer garments including coats/jackets and hats vary.

From a distance, [redacted] saw [redacted] walking on the flight line toward the MPA but outside the marked restricted area. She noticed his distinctive hat but until she talked with [redacted] in the passenger terminal, she did not realize or suspect [redacted] did not have a restricted area badge and that he should not have been on the flight line. After comparing notes with [redacted] and realizing that [redacted] should not have been on the flight line, [redacted] did the right thing and immediately contacted the BDOC.

[redacted], was instructing an [redacted], at the CSO position on the aircraft when [redacted] boarded the aircraft. The airmen on the aircraft should have identified that [redacted] did not have a restricted area badge and notified security forces. According to 89 AW leadership, [redacted] walked confidently past both aircrew members and proceeded to the back of the aircraft. Both [redacted] and [redacted] said they saw [redacted] enter the aircraft and proceed to the back of the aircraft. They said a few minutes later they saw him exit the aircraft. According to [redacted], [redacted] did not say anything when he entered the aircraft, and neither aircrew member communicated with [redacted] while he was on the plane. Both aircrew members were focused on training and did not recognize that [redacted] was not wearing a RAB and did not challenge him or notify anyone regarding his presence on the aircraft.

The nature of the mission of the 89 AW, namely DV airlift, and the environment on JBA present unique challenges for flight line security. There are a large number of civilians with access to the flight line, including civilian aircraft maintenance and 35 identified entry control points to the flight line. Even military aircrew often fly in civilian clothes. During the review team's short tour of the airfield, a civilian was seen exiting an 89 AW C-40 aircraft on the parking ramp to take pictures of the aircraft. Security Forces responded immediately to the situation, but this clearly illustrated the difficulty of identifying personnel and maintaining security on the flight line.

Conclusion

An undetected system malfunction of the FLECS gate at ECP [redacted] allowed an unauthorized civilian to access the JBA flight line on 4 Feb 21. Because the flight line adjacent to ECP [redacted] is considered a [redacted]. The FLECS gates, like the one at ECP [redacted], play a key role in flight line security; however, [redacted]. To be effective, they must present a physical barrier to entry into the controlled area. When ECP [redacted] was left partially open, this physical

barrier became ineffective, [redacted]. Once on the flight line, human errors/limitations enabled [redacted] to remain on the flight line without a RAB, enter the 89 AW MPA restricted area, and eventually board an aircraft without being challenged.

JBAI 31-101 states "[redacted] On 4 Feb 21, the combination of FLECS, Security Forces posts/patrols, and Owner/User personnel failed to adequately protect the flight line and associated aircraft.

AIRCRAFT ACCESS - PL-3 & 89 AIRLIFT WING MASS PARKING RAMP

STANDARDS

AFI 31-101

4.9. [redacted]

4.9.1. [redacted]

4.9.1.1. [redacted]

4.9.1.2. [redacted]

4.9.1.3. [redacted]

4.9.2. [redacted]

5.2. [redacted]

5.2.1. [redacted]

5.2.1.1. [redacted]

5.2.1.2. [redacted]

5.2.1.3. [redacted]

5.2.1.4. [redacted]

5.2.1.4.1. [redacted]

5.2.1.4.2. [redacted]

5.2.1.4.3 [redacted]

5.2.1.4.4 [redacted]

5.3. [redacted]

5.3.1. [redacted]

5.3.1.1. [redacted]

5.3.1.2. [redacted]

5.3.1.3. [redacted]

5.3.1.3.1. [redacted]

5.3.1.3.2. [redacted]

5.3.1.3.3. [redacted]

5.3.1.3.4. [redacted]

5.4. [redacted]

5.4.1. [redacted]

5.4.1.1. [redacted]

5.4.1.2. [redacted]

5.4.1.3. [redacted]

5.4.1.3.1. [redacted]

5.4.1.3.2. [redacted]

5.4.1.4. [redacted]

7.7.1. [redacted]

7.7.2. [redacted]

Excerpts out of JBA's IDP:

[redacted]

[redacted]

[redacted]

[redacted]

ANALYSIS

[redacted] Aircraft Protection (PL-1) and PL-2 Resource Protection

The attention generated by the 4 Feb 21 incident was intensified by the 89 AW's mission and the fact that [redacted] was able to board a "blue and white" 89 AW aircraft. [redacted]. Before addressing the factors that contributed to [redacted] gaining access to the C-40 aircraft, we need to discuss the security surrounding the Protection Level-1 (PL-1) [redacted] aircraft and the difference between that security and the security around a PL-3 C-40 aircraft.

Both PL-1, like the [redacted], and PL-2, like the [redacted] aircraft, have more layers of protection than PL-3 resources like the 89 AW C-40 aircraft. This starts with more robust entry control points that are manned by armed entry controllers. [redacted]

After assessing the PL-1 and PL-2 security postures on JBA, the review team is confident that events similar to what occurred on 4 Feb 21, that resulted in access to the PL-3 resource, would not have resulted in access to a PL-1 or PL-2 aircraft. [redacted].

4 Feb 21 events – Unauthorized Access to a C-40

On 4 Feb 21 an unauthorized civilian walked across a red line into the 89 AW MPA designated restricted area, and then walked up a staircase onto an open PL-3 aircraft without being challenged or detained. After exiting the aircraft, the civilian was intercepted and detained by Security Forces before he could exit the restricted area.

Air Force policy establishes the expectation that PL-3 aircraft will be protected by an intrusion detection capability that is capable of detecting intruders before the intruder enters the PL-3 restricted area and gains access to any PL-3 resources. In this case, the intrusion detection capability was not adequate and failed to identify an unauthorized civilian intruder, [redacted], before he gained access to the restricted area and boarded an aircraft.

Once the BDOC was alerted of a possible intruder on the flight line, the response was excellent. The ramp Security Forces responded, with [redacted] being intercepted and detained immediately after leaving the aircraft, less than two minutes after the BDOC was alerted. The Security Forces Defenders appropriately secured the area, escorted [redacted] outside the restricted area, and effectively detained the individual.

There is lack of clarity in AFI 31-101, section 5.4.1 regarding Owner/User security responsibilities and Security Forces responsibilities when it comes to providing security of PL-3 resources. The section identifies [redacted]. Finally, the section does not clarify who or how IDS capability will be provided when automated IDS capability is not present.

Section 4.9.2 and section 7.7.2 of AFI 31-101 also discuss and differentiate Security Forces' responsibilities and Owner/Users' responsibilities regarding PL-3 security. [redacted]

As discussed in the flight line access portion of this report, [redacted]. Once [redacted] accessed the flight line, there was no automated IDS capable of detecting him prior to entry into the 89 AW MPA restricted area.

316 WG leadership clarified that the 316 SFG did not consider the 89 AW MPA a standard PL-3 restricted area [redacted] to provide intrusion detection at the restricted area boundary fell on the Security Forces. [redacted] According to leadership, this layer of security goes beyond the security requirements for PL-3 areas described in the AFIs, is always present on the 89 AW MPA, and Security Forces personnel are fully aware of this additional security expectation. A written work shift scheduled, titled "the SFS Post Priority Chart" and provided by 316 SFG leadership, confirmed [redacted] teams of Defenders were posted on the 89 AW MPA 24/7; however, the specific roles and responsibilities the Defenders were expected to fulfill while posted on the MPA were not codified in local written guidance.

In summary, written guidance does not definitively identify who is responsible for providing the required intrusion detection capability capable of identifying intruders before they access a PL-3 restricted area and could be interpreted as a shared responsibility between SF and the 89 AW. . Unique procedures at JBA result in a [redacted] team of Security Forces Defenders always being present on the 89 AW MPA when PL-3 resources are located on the ramp. [redacted]

On 4 Feb 21, one 89 AW PL-3 asset, a [redacted], was parked, closed and unoccupied, on the north row of the MPA, while one 89 AW PL-3 asset, the C-40 aircraft accessed by [redacted] was parked in the south east corner of the MPA with 89 AW personnel onboard conducting training. These were the only two PL-3 assets in the designated restricted area. A [redacted] team of Defenders was posted on the 89 AW MPA ramp and positioned to monitor the restricted area entry point and the closed aircraft located on the north end of the ramp. Based on the leadership conversations, the Defenders knew they had intrusion detection responsibility for the entire restricted area. The Owner/Users, in this case two 89 AW aircrew, were present on the open aircraft and understood they had security responsibilities at the aircraft.

On 4 Feb 21, the [redacted] Security Forces team on the MPA should have observed and intercepted [redacted] prior to him reaching the aircraft. However, they were parked in a location where their vision of the south end of the ramp was blocked and they could not observe the entire restricted area boundary. Based on the position of their truck, the Defenders were not focused on providing intrusion detection capability for the entire 89 AW MPA. The fact that they did not observe [redacted] and calmly walk the 500 to 750 feet across the ramp to the C-40 aircraft supports this conclusion.

The two 89 AW personnel who were on the aircraft on 4 Feb 21 should have challenged [redacted] when he entered the aircraft without a RAB. However, they were not equipped or expected to provide intrusion detection before [redacted] reached the aircraft. [redacted] Furthermore, OG leadership emphasized the importance of having a safe space for aircrew to accomplish training on the ramp while at home station. On the aircraft, the 89 AW personnel were focused on training, and while they observed [redacted] getting on the aircraft, they did not notice he was not displaying a RAB. Given the location of the aircraft, parked on home station, inside a restricted area, on a fully enclosed flight line, and [redacted] general appearance, dark blue pants and jacket, it was reasonable for the aircrew members to be focused on training and fail to identify that [redacted] did not have a RAB.

Since the incident, the Security Forces teams posted on the 89 AW MPA ramp have been directed to move their truck [redacted] when aircraft are present on the MPA ramp. By moving [redacted], the Defender's vision of the restricted area is not blocked [redacted]. This change enables the Security Forces personnel to see the entire MPA ramp and thus provide intrusion detection for the entire restricted area. In addition, the 89 AW has reinforced the Owner/Users' responsibilities regarding providing security for 89 AW assets. Given the heightened security environment present following the 4 Feb 21 incident, it is unlikely another intruder could enter the MPA and board an aircraft undetected. However, over time this security awareness may wane, and without clear codified guidance that effectively delineates who is responsible for intrusion detection for PL-3 resources on the 89 AW MPA, the chance of another [redacted] like event may increase.

Conclusion

Human errors and limitations contributed to [redacted] gaining unauthorized access to a PL-3 designated C-40 aircraft parked on the 89 AW MPA on 4 Feb 21.

A sequence of events and failures on 4 Feb 21 led to [redacted] entering a restricted area without being detected and boarding an 89 AW aircraft without being challenged. Security Forces personnel were present and should have seen [redacted] and intercepted him before he accessed any resources. 89 AW personnel on the aircraft should have challenged [redacted] when he boarded the aircraft without a RAB, but they were focused on training with a reasonable expectation of security while parked inside a restricted area.

Air Force guidance clearly establishes the expectation that PL-3 assets will be protected by an intrusion detection capability capable of detecting intruders before the intruders gain access to the resource. On 4 Feb 21, that intrusion detection capability failed.

The 4 Feb 21 incident highlighted a clarity issue in Air Force guidance regarding Owner/Users security responsibilities and Security Forces responsibilities when it comes to providing intrusion detection capability for PL-3 restricted areas. Although local procedures at JBA mitigated the direct impact of this clarity issue, [redacted] was still able to access a PL-3 asset inside a PL-3 restricted area on the 89 AW MPA. Air Force leadership at all levels should consider if current written guidance adequately delineates who is responsible for providing intrusion detection regarding PL-3 resources. Based on the response and interest generated by the 4 Feb 21 incident, Air Force leadership should also consider if the 89 AW MPA ramp should be designated a PL-2 area.

While the 4 Feb 21 event occurred at JBA, [redacted] JBA is not unique when it comes to having to protect PL-3 assets with limited resources. The Air Force should consider if current guidance adequately addresses the issue of intrusion detection surrounding PL-3 resources beyond JBA as well, and specifically assess if similar clarity issues exist in PL-1 and PL-2 security guidance.

V. SUMMARY

On 4 Feb 21, a combination of human errors and limitations, system malfunctions, and unique JBA mission requirements culminated in [redacted], an unauthorized civilian: (1) accessing and remaining on a high profile Air Force installation; (2) gaining unauthorized access to a controlled area, in this case the flight line; and (3) ultimately entering a restricted area undetected and boarding an Air Force aircraft without being challenged.

Initially, human error at a single point of failure led to [redacted] accessing the base. In this case a fully qualified and trained [redacted] SFS defender serving as a gate guard got complacent and did not follow procedures. If the SFS defender had followed normal procedures, [redacted] would have been turned around at the gate and never allowed access to the base. Once on the base, there was no capability to monitor [redacted] actions and no reason to question if he was authorized to be on base.

An undetected system malfunction of the [redacted] at ECP [redacted] allowed [redacted] to access the JBA flight line. The flight line adjacent to ECP [redacted] is [redacted], and the ECP [redacted] gate provides a physical barrier that protects the controlled area. When the gate malfunctioned and remained partially open, this physical barrier became ineffective, [redacted]. Later, when the malfunction at ECP was identified, the gate was quickly secured.

JBA mission requirements and human error allowed [redacted] to stumble on a gap in security and gain access to an aircraft. On 4 Feb 21, two aircraft were parked on the 89 MPA ramp. One of the aircraft was being used for training and occupied by two enlisted aircrew members from the 89 AW and thus was open with air-stairs attached. Security Forces members were positioned on the ramp but were focused on the north end of the restricted area and did not

see [redacted] and enter the restricted area. The aircrew members, who were in a training mindset on their home station and not focused on providing intrusion detection for the aircraft, failed to challenge [redacted] when he entered the aircraft.

During a discussion at the passenger terminal two astute Air Force members pieced together that [redacted] had possibly accessed the flight line without a line badge and alerted the BDOC of a possible unauthorized person on the flight line. As soon as Security Forces was notified about a potential of unauthorized civilian on the flight line, their response was excellent. Security Forces responded immediately, and [redacted] was intercepted and detained in less than two minutes.

The chain of events that led to [redacted] gaining access to an 89 AW aircraft could have been interrupted and prevented earlier at multiple points. If the gate guard had initially followed normal procedures, [redacted] would not have been allowed on base. If the ECP [redacted] malfunction had been identified earlier, [redacted] would not have been able to access the flight line. If personnel on the flight line had identified that [redacted] did not have a RAB or observed him crossing the red line, he would have been detained before accessing the aircraft.

Finally, there is no evidence [redacted] intended to cause harm to Air Force personnel or equipment, and at no time was the security of a [redacted] Aircraft threatened.