National Aeronautics and Space Administration

NASA COUNTERINTELLIGENCE

Fall 2013

Informational Newsletter on Counterintelligence and Counterterrorism Issues Affecting NASA

Message from Joseph S. Mahaley, NASA Assistant Administrator for Protective Services

Maximizing our Agency's counterintelligence/counterterrorism (CI/CT) effectiveness is even more important today than it was when I wrote my first message for last year's *NASA CI Newsletter*. Over the past few months, we have seen an increasing number of media reports concerning the wide variety of cyber and espionage threats arrayed against the U.S. Government and its contractors by foreign governments as well as nonstate actors. NASA and its contractors are not immune to these threats. To the contrary, because of the research and projects that our Agency conducts, NASA is one of the most attractive targets for those who are determined to steal America's technology not only for financial and ideological gain but also to do harm to our country.

It is for this reason that all of us at NASA, civil servants and contractors, need to be constantly mindful of these threats to our Agency and our Nation and do our utmost to identify and counter them. In the past year, I've had the opportunity to visit every major NASA facility and meet hundreds of employees. I've seen firsthand that NASA's workforce is composed of hard-working, exceptionally talented individuals who endeavor to protect our technology and our infrastructure. It is our mission to ensure that they have the protections in place to help them to succeed.

As NASA's senior intelligence, counterintelligence, and security official, I place a strong emphasis on the CI/CT Program. In fact, one of my first priorities as the incoming Assistant Administrator for Protective Services was to initiate a 5-year CI/CT expansion plan to address the ever-increasing threat from CI/CT activities. To date, this has resulted in the hiring of several CI Special Agents detailed to our Centers and a CI Cyber Analyst here at NASA Headquarters. Despite the challenges imposed by budgetary limitations, I am committed to pursuing our expansion and improvement of this vital program.

In closing, I want to take this opportunity to thank you, our frontline CI professionals, for your dedication to keeping NASA's people and property safe. I want you to know that your continuing diligence and outstanding efforts are appreciated by NASA's senior leadership. Thank you for the exceptional work you do for our Agency and for the United States of America.

Who in Cyberspace Is Viewing, Collecting, and Responding to Your Thoughts?

A NASA employee experienced two unusual and unexpected response "tweets" to generic information posted via Twitter by the employee while she was recently on official foreign travel. The employee experienced this issue in different countries, and both instances were unexpected. This employee, like so many at NASA, is excited and electrified by NASA and the work the Agency does, and she regularly tweets her opinions

Continued on next page

Office of Protective Services

Assistant Administrator
Joseph S. Mahaley
202-358-3752

(b) (7)(E)

Counterintelligence/ Counterterrorism Division

Director
(b) (6), (b) (7)(C)

Operations
(b) (6), (b) (7)(C)

(b) (6), (b) (7)(C)

Cyber Analyst
(b) (6), (b) (7)(C)

Administrative Assistant
(b) (6), (b) (7)(C)

Counterintelligence Quote

"Foreign attempts to collect U.S. technological and economic information by cyber espionage will continue at a high level in 2012 and will represent a growing and persistent threat to U.S. economic security."

—*Antone Gonsalves,* InformationWeek

and thoughts, as well as events happening at NASA, via Twitter and other social media.

The first event occurred after the NASA employee posted a picture, via Twitter, of the view from her hotel room with no geographical tags or location finders. Almost immediately, she received a response to the tweet, from someone in a neighboring hotel, commenting on her post and hoping she was enjoying her stay. This was alarming to the employee because she had not tagged the location in the photo and because the response tweet was generated from a hotel down the block from where she was staying. The employee did not respond to the tweet.

The second incident occurred in the same fashion: during the employee's official travel, but in a different country. The employee was in the country's airport and tweeted an off-the-cuff remark about needing coffee. Within seconds of the tweet, a response from inside the airport showed her multiple coffee shops located throughout the airport terminals. Although this was helpful in her search for coffee, the tweet made the employee contemplate that all information released into cyberspace is information for anyone to view, collect, and act upon. The remarks tweeted were of little or no consequence; however, the responses to them brought home the lesson that you do not know who is out there in cyberspace.

NASA Counterintelligence Perspective
NASA is an information-sharing agency that collaborates with many nations around the world in research, technology, information, and missions; however, the NASA community needs to keep in mind that each person with a NASA badge has been entrusted with safeguarding sensitive, proprietary, and (in some cases) classified material.

In accordance with NASA Policy Directive 1660.1B, the employee who received the tweets showing knowledge of her location reported the incidents because she thought that her experience might raise potential security concerns for others in the Agency. Vigilance is the best single defense in protecting information, operations, facilities, and people.

Please report counterintelligence-related incidents or issues to your local NASA Counterintelligence office.

Possible Foreign Intelligence Surveillance of a NASA Employee While on Official Overseas Travel, As Well As Useful Countermeasures

During recent official overseas travel to a country that, historically, has engaged in aggressive intelligence collection against the United States and NASA, a NASA employee experienced two suspicious/unusual events indicative of possible host-nation intelligence service targeting.

In the first instance, while looking for an item in an outer, zipped pocket of a piece of luggage he had left in his hotel room, the NASA employee discovered that his RSA token (which he had stored in that outer luggage pocket) had been detached from the lanyard that he normally used to carry the token. The employee found this highly unusual since the token was not easy to remove from the lanyard.

The second suspicious event occurred when the employee returned to his hotel room earlier that had originally been planned. As he approached his room, he saw a housekeeper who appeared alarmed at his early return and ran up to him with the television remote from his room. The employee believed the housekeeper was almost in a panic that he would return to his room without the remote being there.

The employee also mentioned observing multiple smoke detectors in hotel rooms he had previously stayed in during official travel to the same country. Other NASA employees have reported similar circumstances.

NASA Counterintelligence Perspective
NASA is a world leader in the research, development, testing, evaluation, and fielding of leading-edge technologies. Our accomplishments awe and inspire the world. As such, the Agency is also a target of foreign intelligence collection. Countries and companies can save substantial amounts of money by stealing technology and can use that stolen information to challenge us culturally, militarily, and economically. Though one may explain away the above events by saying that the token was separated from its lanyard due to jostling during travel, that the housekeeper may have changed the batteries in the remote to ensure that the guest had a properly working remote, and that the country visited is just security-conscious when it comes to fire prevention, it is also likely that these events were related to host-nation intelligence targeting of this NASA employee.

The bottom line is this: When traveling overseas, in particular for official business and where accommodations are provided by the host, assume that your hotel room and work spaces contain clandestine audio and video surveillance devices.

NASA Center CI Offices

Ames Research Center:
(b) (6), (b) (7)(C)

Dryden Flight Research Center:
(b) (6), (b) (7)(C)

Glenn Research Center:
(b) (6), (b) (7)(C)

Goddard Space Flight Center:
(b) (6), (b) (7)(C)

Jet Propulsion Laboratory:
(b) (6), (b) (7)(C)

Johnson Space Center:
(b) (6), (b) (7)(C)

Kennedy Space Center:
(b) (6), (b) (7)(C)

Langley Research Center:
(b) (6), (b) (7)(C)

Marshall Space Flight Center:
(b) (6), (b) (7)(C)

Stennis Space Center:
(b) (6), (b) (7)(C)

CI Home Page Web Site:
(b) (7)(E)