National Aeronautics and Space Administration

Headquarters
Washington, DC 20546-0001

February 18, 2016

Reply to Attn of: OLIA/2016-00059:JG:eel

The Honorable John Thune
Chairman
Committee on Commerce, Science and Transportation
United States Senate
Washington, DC 20510

Dear Chairman Thune:

Thank you for your letter with regard to an alleged cyber attack by the hacker group AnonSec. We share your concerns about this matter and take any allegation of a cyber attack seriously at the highest levels of the Agency.

We are pleased to report that after extensive analysis, NASA has found no credible evidence of compromise of NASA systems or exfiltration of sensitive data, as alleged by AnonSec. Therefore, we hope that the attached responses to your questions are helpful in ensuring you that NASA has taken these allegations very seriously and has worked diligently and expeditiously to disprove the hacker's claims. Per your request, we also have scheduled meetings in the near future with your staff to discuss this matter in more detail.

Please be assured that NASA works constantly to ensure that its Information Technology (IT) systems and their associated components are safeguarded from attack, assessed against stringent Federal and Agency security requirements, and continuously monitored for compromise and for the effectiveness of protective measures. Should allegations or evidence of a threat occur, NASA has a very mature response process for handling and resolving these threats. This process is led by the NASA Security Operations Center (SOC), which includes key participants from NASA Headquarters and the Centers. The SOC's embedded threat team also has direct ties to the Intelligence Community, the Federal Bureau of Investigation and the U.S. Computer Emergency Readiness Team.

We appreciate your ongoing interest in this important matter, and we appreciate your strong support for NASA.

Sincerely,

Seth Statler

L. Seth Statler
Associate Administrator
for Legislative and Intergovernmental Affairs

Enclosure

Enclosure
February 17, 2016

NASA Responses to Questions 1-7

Please note that all information is current as of February 17, 2016.

1. **Did any aspect of this alleged intrusion occur? If so, when?**

NASA Response:

After extensive investigations by the NASA Security Operations Center (SOC) analysts, Center Security officials, and Agency Center security responders, we have identified no credible evidence of compromise of NASA systems, or exfiltration of sensitive data, as alleged by the hacker group, AnonSec. Although NASA's investigation is ongoing, we are increasingly confident that the purportedly "hacked" data were publicly available prior to the supposed intrusion.

Initially, AnonSec's claims appeared credible due to carefully crafted references to real people, systems, projects, and large quantities of publicly available data. However, their statements were devoid of specific timelines thereby making NASAs investigation into their claims challenging to disprove. Still, every investigative path taken by NASA's security team thus far has led to evidence refuting or disproving the claims made by AnonSec.

2. **If so, when did NASA officials, including, but not limited to, the Chief Information Officer, Security Operations Center personnel, and the OIG, first become aware of the intrusions**

NASA Response:

NASA first became aware of hacking claims by AnonSec on Jan. 29, 2016. NASA CIO, SOC personnel, and the Office of the Inspector General (OIG) were notified the same day.

As noted earlier, no credible evidence of compromise of NASA systems or exfiltration of sensitive data, as alleged by AnonSec, has been identified after extensive analysis.

3. **If it did occur, how long did the hackers have access to NASA networks? Were the hackers able to exfiltrate sensitive agency data? If so, how much?**

NASA Response:

No credible evidence of compromise of NASA systems or exfiltration of sensitive data, as alleged by AnonSec, has been identified after extensive analysis.

4. What steps has the agency taken to mitigate the potential risk to critical NASA systems targeted by the alleged intrusion?

NASA Response:

NASA works constantly to ensure that its Information Technology (IT) systems and their associated components are safeguarded from attack, assessed against stringent Federal and Agency security requirements, and continuously monitored for compromise and for the effectiveness of protective measures. Should allegations or evidence of a threat occur, NASA has a very mature response process for handling and resolving these threats. This process is led by the NASA SOC, which includes key participants from NASA Headquarters and the Centers. The SOC's embedded threat team also has direct ties to the Intelligence Community, the Federal Bureau of Investigation and the U.S. Computer Emergency Readiness Team.

With regard to the AnonSec claims, the Agency conducted an extensive review and no credible evidence of compromise of NASA systems or exfiltration of sensitive data, as alleged by AnonSec, has been identified after extensive analysis. While NASA is continuously evaluating its systems' security, because there is no evidence of an actual breach, there are no new risks to mitigate or steps to consider as a result of this specific event.

5. Has NASA informed affected employees regarding the exposure of their personal details? Has NASA provided assistance to these employees?

NASA Response:

There was no exposure of NASA employee personal details. Employee names and official contact information were included in the alleged compromised data; however, this information is available publically through many sources including the website: https://people.nasa.gov. Accordingly, no employee notifications have been made.

6. Has NASA informed appropriate federal agencies, including, but not limited to the FBI, the Department of Homeland Security, and the Executive Office of the President if the incident occurred and its extent?

NASA Response:

As there has been no credible evidence of compromise of NASA systems or exfiltration of sensitive data, this was not reported as an incident through the U.S. Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT) reporting process. NASA did, however, share information related to this event on Feb. 4, 2016, with participants on the US-CERT's weekly conference call. NASA is also working with the OIG on details pertaining to this event.

7. How is NASA addressing open OIG recommendations regarding information security?

NASA Response:

NASA has made significant progress closing OIG issued recommendations since 2010. Of the 75 recommendations received, NASA has closed 65. The Agency is currently working to close

10 open OIG recommendations. Ongoing efforts to close open OIG recommendations include a wide breadth of activities such as modifying current policies to reflect new requirements, implementing Continuous Diagnostics and Mitigation (CDM), and utilizing Personal Identity Certification (PIV) solutions.

United States Senate

COMMITTEE ON COMMERCE, SCIENCE,
AND TRANSPORTATION

WASHINGTON, DC 20510–6125

WEBSITE: http://commerce.senate.gov

February 10, 2016

The Honorable Charles F. Bolden, Jr.
Administrator
National Aeronautics and Space Administration
300 E Street SW
Washington, D.C. 20546

Dear Administrator Bolden:

Recent reports indicate that NASA may have suffered a significant cyber attack, in which hackers gained broad access to NASA networks and exposed sensitive information. If these reports are accurate, hackers exploited vulnerabilities in system administrator credentials to gain access to the agency's networks over the course of several months. The information allegedly released may include more than 600 aircraft and radar videos, more than 2,000 flight logs, as well as the personal details of nearly 2,500 NASA employees. In addition, after gaining access to the agency's networks, hackers claim to have attempted to crash the Global Hawk, a NASA-operated aircraft costing approximately $200 million, into the Pacific Ocean before being shut out of the network.

In responding to these press reports, NASA officials have insisted that the hackers' claims of access to, and control of, the Global Hawk were false. In addition, NASA officials have maintained that much of the data the hackers claim to have accessed and released was already publicly available. The agency, however, has not verified that all of the released information was publicly available, nor has it ruled out the possibility that this intrusion did in fact occur.

I recognize that the claims of the hackers may be overstated or fabricated, and hope that they are. Nevertheless, the possibility of such an intrusion is particularly disconcerting in light of prior incidents at NASA. For example, in 2012, the NASA Office of Inspector General (OIG) reported that 13 advanced persistent threat attacks successfully compromised NASA's computers in fiscal year 2011. One incident at the Jet Propulsion Laboratory (JPL) involved full functional control over key JPL systems and sensitive user accounts. In addition, stolen laptops in past years have resulted in the loss of the algorithms used to control the International Space Station, sensitive data on NASA programs, and personally identifiable information. Furthermore, NASA is a target-rich environment for cyber attacks, and reported more than fifteen thousand security incidents to the Department of Homeland Security in fiscal year 2014, more than any other agency reporting under the Chief Financial Officers Act.

The scope of the latest alleged intrusion, the sensitivity of the information in question, and NASA's recent history of other cyber attacks raise serious concerns about NASA's ability to secure information and protect its networks from future attacks. Moreover, the NASA OIG has identified the need for improvement of information technology security as a priority for the agency. Therefore, in order to assist the Committee with its oversight duties, please provide the following information:

1. Did any aspect of this alleged intrusion occur? If so, when?

2. If so, when did NASA officials, including, but not limited to, the Chief Information Officer, Security Operations Center personnel, and the OIG, first become aware of the intrusion?

3. If it did occur, how long did hackers have access to NASA networks? Were the hackers able to exfiltrate sensitive agency data? If so, how much?

4. What steps has the agency taken to mitigate the potential risk to critical NASA systems targeted by the alleged intrusion?

5. Has NASA informed affected employees regarding the exposure of their personal details? Has NASA provided assistance to these employees?

6. Has NASA informed appropriate federal agencies, including, but not limited to, the FBI, the Department of Homeland Security, and the Executive Office of the President if the incident occurred and its extent?

7. How is NASA addressing open OIG recommendations regarding information security?

Please provide the requested information as soon as possible, but by no later than February 24, 2016. In addition, please direct your staff to make arrangements to brief Committee staff on this matter by no later than February 16, 2016. If you have any questions, please contact Ashok Pinto or Suzanne Gillen of the Majority staff at (202) 224-1251. Thank you in advance for your prompt attention to this matter.

Sincerely,

JOHN THUNE
Chairman

cc: The Honorable Bill Nelson
Ranking Member

The Honorable Ted Cruz
Chair
Subcommittee on Space, Science, and Competitiveness

The Honorable Gary C. Peters
Ranking Member
Subcommittee on Space, Science, and Competitiveness

The Honorable Kelly A. Ayotte
Chair
Subcommittee on Aviation Operations, Safety, and Security

The Honorable Maria Cantwell
Ranking Member
Subcommittee on Aviation Operations, Safety, and Security

The Honorable Paul K. Martin
Inspector General
NASA