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

Current Terrorist Threat Condition
No Active Alerts

NASA CI/CT MONTHLY NEWS UPDATE – August 2015

This monthly newsletter is published to increase NASA personnel awareness of significant current issues related to counterintelligence, counterterrorism, and counterintelligence cyber matters. To learn more about CI/CT awareness, or to schedule a CI/CT presentation, please contact the CI POC located on the last page.

Significant Counterterrorism (CT) Issues:

ATTORNEY GENERAL SAYS ISIS IS MORE OF A THREAT THAN AL QAEDA

The Attorney General (AG) says the threat from ISIS is so great because the terror group's technologically advanced tactics are "still new to us," and the U.S. government is "still trying to determine the scope" of efforts to radicalize Americans and others worldwide.
http://abcnews.go.com/Politics/attorney-general-isis-threat-al-qaeda/story?id=32691727

CHATTANOOGA ATTACK MISSED BUT U.S. FOILED 'OVER 60' ISIS PLOTS

Three days after four marines and a sailor were killed by a gunman with Middle Eastern roots, the chairman of the House homeland security committee heralded US successes against "over 60" would-be terrorist attacks by "ISIS followers" in the last year.
http://www.theguardian.com/us-news/2015/jul/19/chattanooga-isis-terror-plots-homeland-security

Significant Counterintelligence Issues:

AMERICAN COMPANIES WARNED OF RISE IN ESPIONAGE

The FBI Assistant Director for Counter Intelligence (CI) said recently at a joint news briefing with the National Counterintelligence Security Center (NCSC) that their intelligence collection activities and investigations indicate "a 53 percent increase, since last year at this time, in the number of economic espionage cases that we're involved in."
http://wtop.com/national-security/2015/07/american-companies-warned-rise-espionage/

ESPIONAGE AND INDUSTRY IN THE INTERNET ERA

Spying may be the world's second-oldest profession, but espionage has been quick to embrace the technology of the internet era. Just as the online economy has made it easier to buy and sell goods and services, so the net is making it easier to steal and trade information.
http://www.ft.com/intl/cms/s/2/01714ea4-262e-11e5-bd83-71cb60e8f08c.html#axzz3fxu5jhgJ

Significant Cyber Issues:

THESE 5 FACTS EXPLAIN THE THREAT OF CYBER WARFARE

America has spent decades and trillions of dollars building up the greatest military force the world has ever seen. But the biggest threat to national security these days comes from not from aircraft carriers or infantry divisions, but a computer with a simple Internet connection. That much became clear after the catastrophic hack—most likely by a foreign power—of sensitive federal employee data stored online.
http://time.com/3928086/these-5-facts-explain-the-threat-of-cyber-warfare/

HACKERS EXPOSE SPY SOFTWARE FIRM'S GLOBAL CLIENTS

A recent breach at an Italian surveillance company has laid bare the details of government cyber-attacks worldwide, putting intelligence chiefs in the hot seat from Cyprus to South Korea. The massive leak has already led to one spymaster's resignation - and pulled back the curtain on espionage in the iPhone age. More than 1 million emails released online in the wake of the July breach show that Hacking Team sold its spy software to the FBI and to Russian intelligence.
http://www.cbsnews.com/news/italy-hacking-team-breach-suggest-spy-software-sold-fbi-russia-vatican/

Analyst Notes – Items to Watch:

The July 16th attack in Chattanooga TN was yet another sign that ISIS has not lost its ability to recruit and inspire "Lone Wolf" attackers in the United States. ISIS influence and power continues to expand in Yemen, Africa, Afghanistan and Russia. The sophisticated use of social media by ISIS remains effective despite mounting efforts by the West to counter it. Al Qaeda (AQ) continues to have increasing success in Syria and in Yemen, with AQ groups expanding their influence despite military pressure. Cyber espionage continues to dominate the news, especially in light of massive data losses suffered by the U.S. government. These data breaches include even more information losses dealing with U.S. government employees than previously thought. The NASA CI/CT division will continue to monitor these threats and any others that emerge in the future that have the potential to harm NASA or its equities.

NASA CI Offices:

Ames Research Center: (b) (6), (b) (7)(C)
Armstrong 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)
NASA Headquarters: (b) (6), (b) (7)(C)
Stennis Space Center: (b) (6), (b) (7)(C)