EIB World Trade Headlines

Evolutions In Business • www.eib.com • (978) 256-0438
Fax: (978) 250-4529 • P.O. Box 4008. Chelmsford. MA 01824

May 15, 2017 - Volume 9, Issue 10

The Head of the Census Resigned. It Could Be as Serious as James Comey

In a week dominated by President Trump's firing of FBI director James Comey, you could be forgiven for missing the imminent departure of another, less prominent federal official.

Yet the news this week that John H. Thompson, the director of the Census Bureau, has abruptly resigned is arguably as consequential to the future of our democracy. That's because the Census Bureau, while less flashy than the FBI, plays a staggeringly important role in both U.S. elections and an array of state and federal government functions.

"At the very heart of the Census is nothing less than political power and money," said Terri Ann Lowenthal, who served as the staff director of the House census oversight subcommittee before becoming a consultant on census policy and operational issues. "It is the basis, the very foundation, of our democracy and the Constitution's promise of equal representation."

*(*Continued On The Following Page)*

NEWSLETTER NOTES

The results of the decennial Census—the next will be in 2020—will determine how state and federal political districts are drawn; which Americans are "counted" for representation; and how federal dollars, many of which are allocated on a per capita basis, are spent.

The Founding Fathers believed so deeply in the importance of a comprehensive census that they included a legal requirement for it in the Constitution, a clause later underscored by the Fourteenth Amendment. We have carried out a national Census every ten years since 1790.

Thompson's early departure has the potential to undermine that tradition. The director's fixed, five-year term had been extended through 2017 and his exit was a surprise. Some advocates speculate he was pushed out for political reasons, although there is no evidence to support that claim.

What's clear is Thompson's resignation leaves the agency in a tough position. During the critical ramp up period before the 2020 Census, the bureau now faces a leadership vacuum, a dearth of funding, and a potentially contentious political fight over the nomination of the next director.

"The timing of Thompson's departure could not be worse," said Phil Sparks, co-director of the Census Project, a non-profit coalition that advocates for a fair Census. "If you're not on schedule with field tests in 2018, it's just not going to go as planned."

There are three big problems with a vacuum of leadership at the bureau at this particular political moment.

The first has to do with maintaining the basic function of the agency, which must follow a strict, 10-year schedule. "The Census is on a relentless calendar. You cannot postpone it," Kenneth Prewitt, who was director of the Census Bureau during the 2000 Census, told TIME. "There's a huge amount of planning and testing to do beforehand. With a leadership vacuum, things slow down."

Lowenthal says she does not expect the Trump administration to nominate a replacement for Thompson this year, and even after that takes place, the Senate confirmation process could take many more months. With so many other vacancies in the federal government, it's possible the role could remain unfilled for the next year or more.

The second big problem facing the agency has to do with money. Without a respected director to push Congress and the White House to give adequate funding to the bureau, the agency risks stumbling on a shoestring budget. In April, Congress allocated just $1.47 billion to the agency, roughly $150 million less than officials believe is necessary at this stage in the 10-year cycle. The President's proposed 2018 budget provides just a minor bump, with $1.5 billion next year.

*(*Continued On The Following Column)*

Without more funding, Sparks says, an interim leader may be forced to make grim choices. He or she may decide, for example, to roll out untested new internet-based programs, increasing the risk of a failure in 2020 (see Healthcare.gov), or to cannibalize other programs, like the annual American Community Survey or this year's economic survey, which is used to inform consequential decisions at the Federal Reserve.

An interim leader might also be forced to give up on an online census entirely, opting instead for the old school pencil and paper version the bureau has used for 220 years—a move that would save money in the short term, but end up costing tax payers, according to the Commerce Department, $5 billion more down the road over the full 10-year cycle.

The third main problem with a vacuum of leadership at the bureau at this political moment is a little more slippery. It has to do, watchdogs say, with the vagaries of public perception. "It is vital, it is critical, that the public has confidence in the integrity of the process and faith in the results," said Lowenthal. "Anything that compromises that, compromises the whole mission."

Prewitt warned that if the agency doesn't receive the funds or political support it needs, it could force a public crisis. "If you underfund the census, you get an undercount," he said. "And if you don't count people, they are politically invisible, in effect." If the 2020 Census appears to undercount certain populations or demographics in certain cities or states, he said, that could discredit the agency's perceived competency. Already, the Census Bureau has scaled back its 2020 advertising budget used to inform Americans about the Census takers who will be coming to their doors.

The public could also lose faith in the legitimacy of the Census results if they are seen to be politicized, Lowenthal said. If President Trump, for example, who has already ridiculed federal statistics and attacked federal institutions, were to "send one errant tweet during the Census calling into question the integrity of the process," she warned, he could do a significant amount of damage, forcing what could become a Constitutional crisis.

It has happened before. After the 1920 Census, members of Congress refused to accept data showing the increasing urbanization of the country, and voted not to reallocate seats based on that supposedly flawed data.

Bruce Bartlett, a former Republican White House and Congressional aide, says it wouldn't be the first time the agency's work became a political hot potato. In 2009, Tea Party Republicans sought to undermine the bureau's credibility by suggesting that its annual American Community Survey, or ACS, was an unreasonable intrusion into Americans' privacy. In 2012, a Republican-led House voted 232 to 190 to abolish the ACS entirely.

*(*Continued On The Following Page)*

In an email to TIME, Bartlett pointed out the damaging effect of a director who was seen to be pulling levers in favor of one political party or another. "The director of the Census makes a lot of important policy decisions about how much effort should be put into tracking down hard-to-find populations that can easily tilt the results," Bartlett wrote. If a new Trump-appointed director was seen as making decisions that had the effect of excluding minorities, undocumented immigrants, or non-English speakers, that could have a ripple effect. The Census results would still be used to reallocate state and federal seats, "shifting representation and money from blue states to red states," Bartlett wrote.

Prewitt said if that sort of scenario played out, it's all over. "If you go down the channel where you're making choices designed to benefit one of the parties," he warned, "you've killed the census."

New Items and Announcements

Industry Notice:

Commodity Jurisdiction Frequently Asked Questions (FAQ) Update: (04.21.17) Frequently asked questions for general information regarding Commodity Jurisdictions (CJ) and the CJ Application Form (DS-4076) have been uploaded.

Key Personnel:

Please Note: Please contact the DDTC Response Team first for all DDTC-related inquiries. The Response Team is set up to address a full range of defense trade inquiries and direct you to a secondary contact, if necessary. The Response Team may be reached at (202) 663-1282 or by email at DDTCResponseTeam@state.gov.

DEPUTY ASSISTANT SECRETARY, DEFENSE TRADE CONTROLS

Brian Nilsson (202) 663-2861

Acting Managing Director

Anthony Dearth (202) 663-2836

Senior Advisor

Glenn Smith (202) 663-2737

Office Management Specialist

YoLanda Mitchell (202) 663-3704

OFFICE OF DEFENSE TRADE CONTROLS LICENSING

Terry Davis	Acting Office Director	(202) 663-2739
Terry Davis	Deputy Director	(202) 663-2739
Demetrice Threat	Administrative Assistant	(202) 663-3234

Division 2 - Plans, Personnel, Programs, and Procedures

Vacant	Division Chief	
David Aron	Senior Analyst	(202) 663-3310
Pete Walker	Senior Analyst	(202) 663-2806

Division 3 - Space, Missile, and Sensor Systems

(USML Commodity Categories IV, V, XII, and XV)

*(*Continued On The Following Column)*

Catherine Hamilton	Division Chief	(202) 663-2839
Jonathan Dennis	Senior Analyst	(202) 663-2734
Yolanda Gantlin	Senior Analyst	(202) 736-9062
Dominic Alford		(202) 663-2990
Alex Douville		(202) 663-2718
MAJ Sean Keefe		(202) 663-2721
George Moose		(202) 663-2793
Edward Pritchard		(202) 663-2745
MAJ Patrick Reimnitz		(202) 663-2719
Kalon Scott		(202) 261-8694
Deniz Smith		(202) 663-2731

Division 4 - Electronic and Training Systems

(USML Commodity Categories IX, XI, XIII, XVI, XVII, XVIII, and XXI)

Angela Brown	Division Chief	(202) 663-2477
Frances Tucker	Senior Analyst	(202) 663-2916
Laurel Bibby		(202) 663-2724
Lisa Brown		(202) 663-2736
David Cavey		(202) 663-2728
Karen Conyers		(202) 663-2738
LTC Timothy Duffy		(202) 663-2804
MAJ Robert Holcroft		(202) 663-2722
Deloris Kinard		(202) 663-2022
Dante Mack		(202) 663-2843

Division 5 - Sea, Land, and Air Systems

(USML Commodity Category II, VI, VII, VIII, XIX, and XX)

Alisa Forby	Division Chief	(202) 663-2798
Mike Boyd	Senior Analyst	(202) 663-3515
CDR Michael Braun		(202) 663-2726
Audra Collins		(202) 663-2982
Angela Gordon		(202) 663-2840
Sebastian Liberatore		(202) 663-2720
Angela McDonald		(202) 663-2735
Lt Col Jaime Sonora		(202) 663-2917
Nicholas Stephenson		(202) 663-3227

back to top

Division 6 - Light Weapons and Personal Protective Equipment Systems

(USML Commodity Categories I, III, X, and XIV)

Chuck Schwingler	Division Chief	(202) 663-2812
Jo-Anne Riabouchinsky	Senior Analyst	(202) 663-2171
Drew Bayliss		(202) 663-2747
Donald Beard		(202) 663-2964
Donald Fanning		(202) 663-3755
LTC Jason Knowles		(202) 663-2733
Julio Santiago		(202) 663-2810
Tom Tinger		(202) 663-2749
Thomas Trotto		(202) 663-2996

*(*Continued On The Following Page)*

Licensing:

One (1) new Name/Address change announcement has been posted. (04.17.17)

Mercury Systems, Inc. Address Change

Effective immediately, Mercury Systems, Inc., 201 Riverneck Road, Chelmsford, MA 01824 will change as follows: Mercury Systems, Inc., 50 Minuteman Road, Andover, MA 018801. Due to the volume of authorizations requiring amendments to reflect this change, the Deputy Assistant Secretary for Defense Trade Controls is exercising the authority under 22 CFR 126.3 to waive the requirement for amendments to change currently approved license authorizations. The amendment waiver does not apply to approved or pending agreements.

All currently approved DSP authorizations identifying Mercury Systems, Inc., 201 Riverneck Road, Chelmsford, MA 01824 will not require an amendment to reflect the change to Mercury Systems, Inc., 50 Minuteman Road, Andover, MA 018801. A copy of this website notice must be attached to the currently approved license by the license holder.

Pending authorizations received by DDTC identifying the old address on the license will be adjudicated without prejudice. A copy of this website notice must be attached to the approved license by the license holder.

New license applications received after May 17, 2017, identifying the old address on the license will be considered for return without action for correction.

All currently approved agreements will require an amendment to be executed to reflect this change. The agreement holder will be responsible for amending their agreement. The executed amendment will be treated as a minor amendment per 22 CFR 124.1(d) and must be submitted as such.

Pending agreement applications that require amending must be brought to the attention of the assigned Agreements Officer by the agreement holder. The necessary changes will be made prior to issuance when the Agreements Officer has been notified.

A copy of this website notice must be maintained by the license holder and presented with the relevant license to U.S. Customs and Border Protection at time of shipment.

*(*Continued On The Following Column)*

Licensing:

One (1) new Name/Address change announcement has been posted. (03.20.17)

Wesco Aircraft Europe Ltd. and Haas Group International SCM Ltd. to Wesco Aircraft EMEA, Ltd. Name Change

Effective April 1, 2017, Wesco Aircraft Europe Ltd. and Haas Group International SCM Ltd. (inclusive of their operating divisions RD Taylor and Fasteq)(collectively Wesco) will change as follows: Wesco Aircraft EMEA, Ltd. (Wesco EMEA). Due to the volume of authorizations requiring amendments to reflect this change, the Deputy Assistant Secretary for Defense Trade Controls is exercising the authority under 22 CFR 126.3 to waive the requirement for amendments to change currently approved license authorizations. The amendment waiver does not apply to approved or pending agreements.

All currently approved DSP authorizations identifying Wesco Aircraft Europe Ltd. and Haas Group International SCM Ltd. (inclusive of their operating divisions RD Taylor and Fasteq) (collectively Wesco) will not require an amendment to reflect the change to Wesco Aircraft EMEA, Ltd. (Wesco EMEA). A copy of this website notice must be attached to the currently approved license by the license holder.

Pending authorizations received by DDTC identifying the old names on the license will be adjudicated without prejudice. A copy of this website notice must be attached to the approved license by the license holder.

New license applications received after April 1, 2017, identifying the old names on the license will be considered for return without action for correction.

All currently approved agreements will require an amendment to be executed to reflect this change. The agreement holder will be responsible for amending their agreement. The executed amendment will be treated as a minor amendment per 22 CFR 124.1(d) and must be submitted as such. New DSP-83s must be executed as a result of the name change, as applicable.

Pending agreement applications that require amending must be brought to the attention of the assigned Agreements Officer by the agreement holder. The necessary changes will be made prior to issuance when the Agreements Officer has been notified.

A copy of this website notice must be maintained by the license holder and presented with the relevant license to U.S. Customs and Border Protection at time of shipment.

*(*Continued On The Following Page)*

Public Comments:

Public comments received on the Notice of Inquiry; Request for Comments Regarding United States Munitions List Category XII. (03.17.17)

USML Category XII Notice of Inquiry
Public Comments
March 15, 2017

Names		Page #	Pages
Analog Devices		2	3
Akin Gump		4	13
BAE Systems		18	4
Clear Align		22	1
DRS Technologies		23	3
FLIR		26	79
Fluke		105	113
George Gasparian		218	2
General Motors		220	2
Harris		222	4
IRP Technologies		226	1
ISP Optics Corporation		227	1
Lakewood Technologies		228	3
Lightpath Technologies		231	1
National Defense Industrial Association		232	3
Nu-trek		235	2
Pembroke Instruments		237	1
Princeton Instruments		238	21
Raytheon		259	9
Resonon		268	3
SA Photonics		271	2
Seiler		273	2
Smithsonian Astrophysical Observatory		275	3
Sofradir-EC		278	4
SPIE		282	4
Thermal		286	9
United Technologies		295	10

For more information **Click here to read**

*(*Continued On The Following Column)*

Web Notice:

DSP-83 Exception Chemical Agent Resistant Coatings (CARC)

UPDATE: DSP-83 Requirement for Licensing of Chemical Agent Resistant Coatings (CARC) Paint

The Directorate of Defense Trade Controls (DDTC) determined that CARC paint does not possess "substantial military utility or capability" as defined by the term Significant Military Equipment (22 CFR 120.7(a)), and therefore does not require a DSP-83 Non transfer and Use Certificate to accompany a license application for the permanent export of the defense article. As a result of a multi- agency review of export controls and the implementation of Export Control Reform (ECR), CARC paint was reassigned as category XIV(f)(7) on the United States Munitions List (USML).

When submitting a DSP-5 via D-Trade, the selection of any SME category in block 11 automatically identifies the defense article as SME and makes the DSP- 83 a mandatory required document. Follow procedures below to submit your application without the DSP-83:

- **Enter "XIV(f)(7)" in Block 11**
- **When asked if a DSP-83 is attached – answer "NO"**
- **When further asked "If SME, and a DSP-83 is not attached, state why." –**
  answer "Updated DDTC Web Notice 2/22/17 ref: no DSP-83 for CARC."
- **Please do not attach a copy of the web notice**

Any questions or concerns should be directed to Chuck Schwingler at schwinglerBC2@state.gov, Supervisory Defense Controls Analyst for the Light Weapons and PPE Systems Division.

Singapore Man Sentenced to 40 Months in Prison for Plot Involving Exports to Iran of U.S. Components

Lim Yong Nam, aka Steven Lim, 43, a citizen of Singapore, was sentenced today to 40 months in prison for his role in a conspiracy that caused thousands of radio frequency modules to be illegally exported from the U.S. to Iran, at least 14 of which were later found in unexploded improvised explosive devices (IEDs) in Iraq.

The announcement was made by Acting Assistant Attorney General for National Security Mary B. McCord, U.S. Attorney Channing D. Phillips of the District of Columbia, Acting Assistant Secretary of Export Enforcement Richard Majauskas for the U.S. Department of Commerce, Acting Director Thomas D. Homan of U.S. Immigration and Customs Enforcement (ICE) and Assistant Director Bill Priestap of the FBI's Counterintelligence Division. The sentence was issued by the Honorable Emmet G. Sullivan.

Lim was extradited in 2016 from Indonesia, where he had been detained since October 2014 in connection with the U.S. request for extradition. He pleaded guilty on Dec. 15, 2016, to a charge of conspiracy to defraud the U.S. by dishonest means. Lim will be deported upon completion of his sentence.

Lim and others were indicted in the District of Columbia in June of 2010 on charges involving the shipment of radio frequency modules made by a Minnesota-based company. The modules have several commercial applications, including in wireless local area networks connecting printers and computers in office settings. These modules include encryption capabilities and have a range allowing them to transmit data wirelessly as far as 40 miles when configured with a high-gain antenna. These same modules also have potentially lethal applications. Notably, during 2008 and 2009, coalition forces in Iraq recovered numerous modules made by the Minnesota firm that had been utilized as part of the remote detonation system for IEDs. According to the plea documents filed in the case, between 2001 and 2007, IEDs were the major source of American combat casualties in Iraq.

In a statement of offense submitted at the time of the guilty plea, Lim admitted that between August 2007 and February 2008, he and others caused 6,000 modules to be purchased and illegally exported from the Minnesota-based company through Singapore, and later to Iran, in five shipments, knowing that the export of U.S.-origin goods to Iran was a violation of U.S. law. In each transaction, Lim and others made misrepresentations and false statements to the 6

*(*Continued On The Following Column)*

Minnesota firm that Singapore was the final destination of the goods; at no point in the series of transactions did Lim or any of his co-conspirators inform the company that the modules were destined for Iran. Similarly, according to the statement of offense, Lim and others caused false documents to be filed with the U.S. government, in which they claimed that Singapore was the ultimate destination of the modules. Lim and his co-conspirators were directly aware of the restrictions on sending U.S.-origin goods to Iran.

Shortly after the modules arrived in Singapore, they were kept in storage at a freight forwarding company until being aggregated with other electronic components and shipped to Iran. There is no indication that Lim or any of his co-conspirators ever took physical possession of these modules before they reached Iran or that they were incorporated into another product before being re-exported to Iran. According to the statement of offense, 14 of the 6,000 modules the defendants routed from Minnesota to Iran were later recovered in Iraq, where the modules were being used as part of IED remote detonation systems.

This investigation was jointly conducted by ICE Homeland Security Investigations (HSI) special agents in Boston and Los Angeles; FBI agents in Minneapolis; and Department of Commerce, Bureau of Industry and Security agents in Chicago and Boston. Substantial assistance was provided by the U.S. Department of Defense, U.S. Customs and Border Protection, the State Department's Directorate of Defense Trade Controls, the Treasury Department's Office of Foreign Assets Control, and the Office of International Affairs in the Justice Department's Criminal Division, particularly the Justice Department Attaché in the Philippines, as well as the FBI and HSI Attachés in Singapore and Jakarta.

U.S. law enforcement authorities thanked the governments of Singapore and Indonesia for the substantial assistance that was provided in the investigation of this matter.

The prosecution was handled by Assistant U.S. Attorney Ari Redbord of the District of Columbia and Trial Attorney Julie Edelstein of the National Security Division's Counterintelligence and Export Control Section.

Fake LinkedIn Emails Phishing Job Seekers

Fake LinkedIn emails are hitting inboxes, trying to get recipients to hand over their CVs.

The scammers are trying to impersonate the popular employment-oriented social networking service, but careful users will immediately spot many things that point to the email being fake:

· The email sender address that has nothing to do with LinkedIn
· The lack of certain design elements and the "unsubscribe" footer usually contained in LinkedIn emails
· The email not addressing the recipient by name
· A sense of urgency that the email is designed to create
· Typos, and so on.

Unfortunately, there are always some users that will fail to spot any of these red flags, and will click on the offered links. They will be taken to a website where they are instructed to upload their CVs. 9

The site (at https://linkedinjobs.jimdo.com) to which the initial emails pointed to has already been taken down, but you can be sure that the scammers have already set up new ones, and changed the link in subsequently sent emails.

"Your CV contains a wealth of personal data which a cybercriminal uses to make a profit at your expense," Heimdal Security's Paul Cucu explains.

"Phone numbers can be sold for companies doing promotional cold calling. Or, the cybercriminal might call you himself in a vishing attack. In other cases, he might use the information for identity theft, using the companies you worked at or attached references as a cover for fraudulent activities."

Or, the scammer could use the info to craft believable spear-phishing emails targeting the person's current or former employers or colleagues.

Total Defense warns about other dangers and typical scams aimed at job seekers:

· Insecure sites (no HTTPS to protect the information inputed into job application forms)
· Follow-up emails soliciting more sensitive information (e.g. bank account number to set up direct deposit)
· Too good to be true job offers that involve a high hourly fee for simple work that can be performed from home
· Non-existing companies contacting users directly with job offers for which they haven't even applied (as in this last LinkedIn scam)

President Trump to arm Syrian Kurdish Forces

President Trump has approved a plan to directly arm Kurdish forces fighting in Syria as part of a U.S. military plan to capture Raqqa, the Syrian city that is the Islamic State's defacto capital, U.S. officials said on Tuesday.

The decision, which was first reported by NBC, is sure to anger Turkey, the NATO ally that views the Kurdish People's Protection Units, or YPG, as a threat and has rebuked the United States for partnering with them in its fight against extremists in Syria.

Two officials, who spoke on the condition of anonymity because the plan had not been announced, confirmed that a decision had been made but declined to provide further details.

The YPG dominates a group known as the Syrian Democratic Forces, which also includes Arab, Christian and Turkmen fighters that have been the Pentagon's premier proxy force fighting the Islamic State in Syria.

While the YPG has received air support from the United States and, indirectly through Arab fighters, some U.S. weaponry, Turkey has warned the United States against arming the group directly. Ankara views the YPG as an extension of the Kurdistan Workers' Party, or PKK, which is considered a terrorist group by both Turkey and the United States.

It was not immediately clear whether the decision by Trump means the YPG will receive heavier weapons, including anti-tank missiles and armored vehicles. Both are likely to be needed if Kurdish troops are to successfully penetrate Raqqa, well-fortified by Islamic State militants.

State Department Employee Arrested and Charged With Concealing Extensive Contacts with Foreign Agents

A federal complaint was unsealed today charging Candace Marie Claiborne, 60, of Washington, D.C., and an employee of the U.S. Department of State, with obstructing an official proceeding and making false statements to the FBI, both felony offenses, for allegedly concealing numerous contacts that she had over a period of years with foreign intelligence agents.

The charges were announced by Acting Assistant Attorney General Mary B. McCord for National Security, U.S. Attorney Channing D. Phillips of the District of Columbia and Assistant Director in Charge Andrew W. Vale of the FBI's Washington Field Office.

"Candace Marie Claiborne is a U.S. State Department employee who possesses a Top Secret security clearance and allegedly failed to report her contacts with Chinese foreign intelligence agents who provided her with thousands of dollars of gifts and benefits," said Acting Assistant Attorney General McCord. "Claiborne used her position and her access to sensitive diplomatic data for personal profit. Pursuing those who imperil our national security for personal gain will remain a key priority of the National Security Division."

"Candace Claiborne is charged with obstructing an official proceeding and making false statements in connection with her alleged concealment and failure to report her improper connections to foreign contacts along with the tens of thousands of dollars in gifts and benefits they provided," said U.S. Attorney Phillips. "As a State Department employee with a Top Secret clearance, she received training and briefing about the need for caution and transparency. This case demonstrates that U.S. government employees will be held accountable for failing to honor the trust placed in them when they take on such sensitive assignments"

"Candace Claiborne is accused of violating her oath of office as a State Department employee, who was entrusted with Top Secret information when she purposefully mislead federal investigators about her significant and repeated interactions with foreign contacts," said Assistant Director in Charge Vale. "The FBI will continue to investigate individuals who, though required by law, fail to report foreign contacts, which is a key indicator of potential insider threats posed by those in positions of public trust."

The FBI arrested Claiborne on March 28. She made her first appearance this afternoon in the U.S. District Court for the District of Columbia.

*(*Continued On The Following Column)*

According to the affidavit in support of the complaint and arrest warrant, which was unsealed today, Claiborne began working as an Office Management Specialist for the Department of State in 1999. She has served overseas at a number of posts, including embassies and consulates in Baghdad, Iraq, Khartoum, Sudan, and Beijing and Shanghai, China. As a condition of her employment, Claiborne maintains a Top Secret security clearance. Claiborne also is required to report any contacts with persons suspected of affiliation with a foreign intelligence agency.

Despite such a requirement, the affidavit alleges, Claiborne failed to report repeated contacts with two intelligence agents of the People's Republic of China (PRC), even though these agents provided tens of thousands of dollars in gifts and benefits to Claiborne and her family over five years. According to the affidavit, the gifts and benefits included cash wired to Claiborne's USAA account, an Apple iPhone and laptop computer, Chinese New Year's gifts, meals, international travel and vacations, tuition at a Chinese fashion school, a fully furnished apartment, and a monthly stipend. Some of these gifts and benefits were provided directly to Claiborne, the affidavit alleges, while others were provided through a co-conspirator.

According to the affidavit, Claiborne noted in her journal that she could "Generate 20k in 1 year" working with one of the PRC agents, who, shortly after wiring $2,480 to Claiborne, tasked her with providing internal U.S. Government analyses on a U.S.-Sino Strategic Economic Dialogue that had just concluded.

Claiborne, who allegedly confided to a co-conspirator that the PRC agents were "spies," willfully misled State Department background investigators and FBI investigators about her contacts with those agents, the affidavit states. After the State Department and FBI investigators contacted her, Claiborne also instructed her co-conspirators to delete evidence connecting her to the PRC agents, the affidavit alleges.

Charges contained in a criminal complaint are merely allegations, and every defendant is presumed innocent until proven guilty beyond a reasonable doubt.

The maximum penalty for a person convicted of obstructing an official proceeding is 20 years in prison. The maximum penalty for making false statements to the FBI is five years in prison. The maximum statutory sentence is prescribed by Congress and is provided here for informational purposes. If convicted of any offense, the sentencing of the defendant will be determined by the court based on the advisory Sentencing Guidelines and other statutory factors.

*(*Continued On The Following Page)*

At her court appearance today, Claiborne pleaded not guilty before the Honorable Magistrate Judge Robin M. Meriweather. A preliminary hearing was set for April 18.

The FBI's Washington Field Office is leading the investigation into this matter. The case is being prosecuted by Assistant U.S. Attorneys John L. Hill and Thomas A. Gillice for the District of Columbia and Trial Attorney Julie Edelstein of the National Security Division's Counterintelligence and Export Control Section.

A Russian Hacker has Created his Own 'Starter Pack' Ransomware Service

Now even low-level criminals can jump into the ransomware game, said the researchers who found the malware.

A new kind of highly-customized ransomware recently discovered by security researchers allows individual criminals to deliver "ransomware-as-a-service".

What sets this ransomware apart from other kinds of file-locking software is that criminals who buy this specialized malware, dubbed Karmen, can remotely control the ransomware from their web browser, allowing the attacker to see at-a-glance a centralized web dashboard of their entire ransomware campaign.

Everything you need to know about ransomware: how it started, why it's booming, how to protect against it, and what to do if your PC's infected.

That dashboard allows the attacker to manage their fleet of infected victims' computers, such as by tracking how much money they've made. If this figure falls short, the attacker can then bump the price of the ransom they seek.

In other words, it's a "starter pack" for low-level criminals to engage in ransomware campaigns, said Andrei Barysevich, director of advanced collection at Recorded Future, who co-authored the report.
"For $175, any script kiddie can carry out ransomware attacks," he said on the phone.

The researchers at Recorded Future, the threat intelligence provider who discovered the malware and have a commercial stake in the space, say that Karmen has been adapted from the abandoned open-source ransomware dubbed Hidden Tear. Besides the fact that it's open source and anyone can use it, the malware itself is unremarkable. It does what it promises: it locks up the victim's files and disks with tough AES-128 encryption, and demands bitcoin as a ransom.

*(*Continued On The Following Column)*

But Karmen adds a modern twist to the abandoned ransomware.

The researchers say that the sole seller of the ransomware, a Russian hacker and developer named "DevBitox" who is motivated by financial gain, created the web-based back-end that makes it easier for attackers to make money.

Each buyer has to set up their own web-based infrastructure, which includes a PHP server running a MySQL database, allowing the attacker to remotely control each infection, like the price of the ransom and the password for each decryption.

DevBitox has also reportedly adapted the open-source malware to include a built-in defense mechanism that detects if the ransomware is run inside a virtual machine, or whether debuggers and analyzing software are found on the system. This then triggers an automatic deletion of the decryptor -- essentially nuking any chance of getting any locked files back.

The seller has probably made a few thousand dollars from what was essentially free ransomware, but he's able to make more, said Barysevich.

"The seller offers some limited support, including up to three file cleanings," he said. Barysevich explained that the buyers will receive the full software package, including the web-based dashboard and the malware used for delivering the ransomware, a tiny 12-kilobyte file that can be attached as an email.
But the hacker will also provide "support" for his product. Because those payload-packed files will periodically get detected by antivirus engines and rejected, each buyer gets three bangs for their buck -- the hacker will rebuild the malicious file to obfuscate it better, and send it along to evade the antivirus engines.

For wider attack campaigns, the individual attacker will need to buy more from the seller. That little bit of money adds on to that "as-a-service," said Barysevich.

So far, only a handful of buyers -- just 20 at the time of writing -- have bought Karmen, according to the researchers, and while three of those have left positive reviews on the seller's profile, their identities aren't known. Ransomware-as-a-service lowers the barrier for criminals to enter the space, and it's only getting more popular.

Earlier this year, the Satan malware allowed low-skilled criminals to carry out ransomware attacks by using someone else's code -- and in return, the developer would take on subscription payments.

Ransomware developers can easily scrape 30 percent return on all revenues generated by cyberattacks. Ransomware rocketed during 2016, costing consumers and business more than $1 billion during the year.

Chinese Hackers go After Third-Party IT Suppliers to Steal Data

The hacking group APT10 has been blamed for the global cyberespionage campaign

Companies that choose to outsource their IT operations should be careful. Suspected Chinese hackers have been hitting businesses by breaching their third-party IT service providers.

Major IT suppliers that specialize in cloud storage, help desk, and application management have become a top target for the hacking group known as APT10, security providers BAE Systems and PwC said in a joint report.

That's because these suppliers often have direct access to their client's networks. APT10 has been found stealing intellectual property as part of a global cyberespionage campaign that ramped up last year, PwC said on Monday.

The joint report doesn't identify which IT service providers were hit or how many were found breached. But the providers included several suppliers in enterprise services and cloud hosting.

"It is impossible to say how many organizations might be impacted altogether at this point," BAE Systems said in a blog post.

APT10 has been around since at least 2009 and is believed to be based in China, according to security researchers. To kick off their attacks, the hackers have used spear-phishing email schemes to trick their victims into installing malware, either through an attachment or through a link that leads to a malicious site.

From there, APT10 will try to steal the credentials from the IT service provider to hop over to their clients' private networks. The hackers will then move on to intellectual property theft, by using the IT service provider's own infrastructure to secretly exfiltrate the data.

APT10's hacking campaign has continued into this year. The group has targeted a whole range of industries across the globe including retail, energy, technology, and the public sector.

The UK's National Cyber Security Centre has warned the public about the hacking campaign. “This incident should remind organizations that entire supply chains need to be managed, and they cannot outsource their risk,” it said in a statement.

Businesses should talk with IT service providers about how they protect access to their data and demand any changes needed, the UK center recommended.

The next billion-dollar startup will be in aerospace

Late last month, 500 people from around the world gathered in Dallas at Uber’s inaugural Elevate Summit.

The invite-only conference was the next actionable step forward, post-Uber’s white paper published last fall, “Fast-Forwarding to a Future of On-Demand Urban Air Transportation,” to catalyze the emerging ecosystem around what Uber, along with partners in aerospace, aviation, and energy storage, see as the next unicorn transportation sector.

On the back of the incredible innovations that have disrupted today’s urban transit systems, with new ride-share models, electric energy and autonomous technologies, urban air mobility is poised for massive growth over the next five years.

At Elevate, with the entire ecosystem gathered in one place, the discussions ranged from identifying key markets and players with commercially viable vehicles to enabling technologies, like battery storage, and aircraft certification and policy, like FAA regulations. After more than 20 years in the aerospace sector, uniting early-stage tech innovators with private capital, my takeaway at the end of this three-day event is that urban air mobility is no longer a future-tech vision… it’s happening now.

It’s only been a few years since we saw the beginnings of a clear renaissance in aerospace.

Early unicorns like SpaceX, OneWeb and Planet radically transformed the landscape, seeding innovations in spacecraft, earth observation, space communication and space exploration, while today next-generation players like Boom, Aurora and Wright Electric are hitting a rapid succession of milestones to bring supersonic jets and regional hybrid aircraft into commercial reality.

Even as I sat between this next generation of Elon Musks and the traditional legacy players, I was amazed to see all the technologies required to bring what many are calling the first flying cars not just to market, but to implementation in what will become an entirely new mode of daily transportation.

The excitement at the event was tangible as we all had the feeling that we are part of something that is going to change the way the world commutes and thus the way we live. Just as autonomous, electric cars will introduce new levels of safety, efficiency and productivity, in this new urban air mobility era, we will spend much less time in transport, in vehicles that will be accessible for most of us and will dramatically reduce the levels of aviation and aerospace emissions.

*(*Continued On The Following Page)*

With Uber pushing the bar, we see a clear business case and a real market for the first commercial vehicle categories. We are shifting from the perception of these as a mere leisure type niche market, relegated to a very small percentage of the population, to opening the way to a much bigger market in terms of the number of vehicles and passengers.

And, as we have a much bigger and commercially viable market, more investors, from angels to VCs to strategics, are entering the game, translating to the kind of money like OneWeb and Planet have benefited from.

Uber, in its role as transit pioneer, has been instrumental in drafting the kind of performance levels required for these future vehicles to operate in a profitable way. It first envisions a varied fleet of urban air vehicles, with an estimated size of 500-1,000 vehicles per city, to carry out the daily trips.

The first model that's emerging is the pool/air/taxi, in which an aircraft will average 24 miles per trip, with 4 passengers, including a pilot (at least in the beginning), that can achieve 150 miles per hour, with 5-minute recharges.

The consensus on the best architecture is a mix of a helicopter and an aircraft, like the Aurora project, which has fixed wings and distributed electrical engines, and the vehicle segment that everyone's talking about, Electric Vertical Take Off and Landing vehicles, eVTOLs, will be part of the class that gets us there. Aurora's fleet is poised to fly this year or next.

Ideally these trips, which will originate at decentralized helipads, will be fully electric solutions that not only drive cost reductions and fuel safety from day one, but also reduce the noise of the vehicle — an ongoing challenge in aviation — to make these more acceptable in urban environments.

On the technology side, the batteries and chargers — already proven in light-, medium- and heavy-duty applications — have the right performance, energy density, capacity and charging time to support frequent, daily trips. With a few expected improvements in coming years, we will see those batteries double their performance in term of size and manufacturing cost, with higher currents and higher power.

Our next steps, post-Elevate, are three-fold. From an infrastructure standpoint, we will reactivate helipads, where in a city like Los Angeles 300 of them already exist but would need to be equipped with electric chargers, and get new authorization to operate in and begin to build charging stations in pioneer cities.

*(*Continued On The Following Column)*

Key to this phase will be ensuring new aircraft certifications tailored to this new class of vehicles are available and, finally, defining the new rules necessary for safe and efficient air traffic management. Though the last may seem daunting, these vehicles should fit in the current traffic as regular general aviation airplane.

The question I was asked more than once over the three days of the conference was "where will we see urban air mobility take flight (and root) first." Though Uber's initial two pioneer cities will be Dallas and Dubai, with partnerships, infrastructure plans, typical routes and regulatory discussions well underway, I see the real disruption taking place in the urban dense, emerging megacities in South America and Asia.

Those regions have already proven their technology ability (and appetite) for leapfrogging to wireless communication systems, and they are once again poised, with their infamously poor and inefficient transit infrastructures, to leapfrog directly to urban air, where the time saved would be tremendous, turning a 1.5 hour drive into a 10-minute flight, 2x/day… for almost the same cost of an UberPOOL.

Solar Impulse Co-founder Aims to Make Electric Aviation a Reality with New Company

Electricity as a vehicle fuel has revealed various benefits. In a day and age where we yearn for both sustainability and efficiency, finding ways to increase energy security, improve fuel economy, lower fuel costs, and reduce emissions has become essential, and electricity does just that. Building on this knowledge, European and Asian countries have been taking advantage of electric high-speed trains for decades. We're also seeing more and more electric cars at affordable prices popping up, too, including the Tesla Model 3. Now, aviation is coming into the picture.

*(*Continued On The Following Page)*

André Borschberg is the co-founder of Solar Impulse, a Swiss long-range experimental solar-powered aircraft project that, just last year, flew electric airplanes for five days and nights nonstop over the Pacific. This marked the longest flight ever of a single pilot airplane. Such success prompted Borschberg to take his electric propulsion technology even further with a new company called H55. The concept behind the venture is to make air transport cleaner, quieter, safer, and — perhaps even more enticing — more affordable!

H55, which will focus on the entire propulsion chain, ranging from the energy source to thrust and power to pilot interface and control systems, has successfully finished 50-plus hours of flight testing already via its electric demonstrator aircraft called the aEro1.

Discussing the prospects of electric propulsion, Borschberg says that "electric air transport will undoubtedly disrupt the aviation industry."

"Fifteen years ago," he continues, "when I started with Solar Impulse, electric propulsion was anecdotal. Today is a major development path of every large aeronautical organisation as well as attracting many start-ups and new players. What is science fiction today will be the reality of tomorrow."

(*Continued On The Following Column)

Web Notice: The Directorate of Defense Trade Controls (DDTC) is currently in the process of modernizing its IT systems. During this time period, we anticipate there may be delays in response times and time to resolve IT related incidents and requests. We apologize for any inconvenience, and appreciate your patience while we work to improve DDTC services. If you need assistance, please contact the DDTC Service Desk at (202) 663-2838, or email at DtradeHelpDesk@state.gov (06.28.16)

"Focus on where you want to go not on what you fear."

The representation of H55 is promising, with co-founders (along with Chairman of the board André Borschberg) including: Sebastien Demont, the former Head of Electrical Engineering at Solar Impulse; Dominique Steffen, a former Red Bull paraglider world champion and experienced Head of Engineering for large-scale projects at Kissling & Zbinden; Thomas Pfammatter, a professional airplane and helicopter pilot with over 10,000 flight hours, former CEO and CFO of Swiss companies, and founder of different start-ups; and Gregory Blatt, former Managing Director for Marketing and External Relations at Solar Pulse.

Let's hope we hear a whole lot more about electric propulsion in the near future, as it offers potentially exciting outcomes. It's extremely efficient and light, for instance, and has flexible and reliable software. Electric airplanes — a cost efficient and therefore less expensive design than the classic combustion aircraft — will also offer far less noise than we're used to, and less environmental impact, too.