The news is rife with warnings of the dangers of Ebola and how easily it can be transmitted, and with fear as contagious as the virus itself, we can readily believe that a terrorist group could somehow capture the virus, inject it into a liquid, and spritz it like a perfume on shoppers in a crowded mall, potentially infecting thousands. Is such a scenario possible?

It may only be in the last several months that the virus has held a prominent position in the news, but actually Ebola has been around for a while and emerged as a suspected biotechnological weapon as early as the 1970s. It is also believed by some that the Ebola virus is a “created” biological weapon. So anything is possible in this sophisticated technological age.

The Japanese cult and future terrorist group Aum Shinrikyo reportedly traveled to the former Zaire in 1992 looking for Ebola samples. There is no evidence they succeeded, but the group did find a way to obtain the deadly gas Sarin and then released that on a Japanese subway in 1995, killing 13. The Ebola outbreak in Uganda in 2012 was viewed as a possible bioterror weapon. Some lawmakers view the currently spreading virus with less concern, but research in the last two years has proven that each time the disease occurs in another place, the strain becomes more deadly.

The Department of Defense considers Ebola to be a viable and not theoretical biological weapon. Although the complicated nature of setting up the virus as a weapon is tricky, effective and efficient dispersion is not impossible. Crude distribution is actually more frightening.

Ebola is transmitted through direct contact with all bodily fluids, so a symptomatic terrorist, sweating heavily hops on and pushes his way a trolley, packed with tourists in San Francisco and...well, you get the picture.

There is a lot of newsprint out there on Ebola as a weapon and our intent in this edition is not to dive into that fray. But the menace of Ebola landing on our shores, and its potential as a bioterrorist’s tool is useful in reminding us that we are a target. We have miles of permeable borderland. So, let’s examine a different, perhaps, more insidious possibility.

We don't think about food defense very often. The grocery store shelves are usually stocked and every year the harvest comes in. It seems unimaginable that life could be different. But consider what would happen if a terrorist introduced widespread contamination among our food animals or released a malicious insect in our fields, severely disrupting our food supply.

Unfortunately, THIS COULD HAPPEN!

We are clearly vulnerable—at every stage of food production and distribution. As the National Infrastructure Protection Plan (NIPP) explains, “...securing this [food and agriculture] sector presents unique challenges because food and agriculture systems in the United States are extensive, open, interconnected, diverse, and they have complex structures...the time required for detection and identification of attacks and contamination, such as animal or plant disease...can be lengthy and complex. Therefore, attacks and contamination...could result in severe animal, plant, public health, and economic consequences.”

An attack on our agriculture would have a significant impact on our lives. The United States Drug Administration (USDA) reports that, in 2012, roughly 9.2% of US employment...
Little skill is necessary in order to produce a deadly but, once done (however crudely), it takes only imagination to find a way to poison or infect the public at the consumption end of the food chain in a relatively short period of time. Only a few well-publicized incidents are needed to instill fear and create panic. Consider these three possible “salad toppers”:

**Bacteria**
In 1984, followers of Bhagwan Shree Rajneesh sprinkled Salmonella Typhimurium on salad bars and in coffee creamers at 10 restaurants in a small Oregon town called The Dalles. Commune members later said they were testing a plan to incapacitate as many residents/voters as possible prior to an important election, the outcome of which was expected to impact their use of the ranch/land they purchased to build a new international headquarters. 751 people got sick, but fortunately there were no fatalities. In addition to the restaurants, produce in at least one supermarket was contaminated and plans were made to also contaminate city water. Rajneesh had set up his own laboratory and investigators discovered there an open vial containing a standard strain of *S* Typhimurium—bought from a commercial supplier of biologic products in Maryland.

*Source: JAMA, August 6, 1997—Vol. 278, No. 5,* from [www.cdc.gov](http://www.cdc.gov)

**Ricin**
In 1978, a Bulgarian dissident was killed a few days after his leg was “injected,” via modified umbrella, with a pin-head sized pellet filled with ricin while standing at a London bus stop. We all know ricin is not difficult to produce, and can be lethal at very small doses. Although filling and firing a pellet that size requires some ingenuity, your basic batch of ricin doesn’t have to be complicated. According to Slate.com, “the entire process can be done in your kitchen, with everyday materials such as coffee filters, mason jars, and solvents found at hardware stores.” Even the castor beans—the key ingredient—are easy to access and recipes for processing your beans are only a click away. Although, according to Slate’s research, your kitchen concoction may not be the highest quality and therefore not as deadly. Still......

**Cyanide**
In 1982, Extra-Strength Tylenol capsules laced with potassium cyanide killed seven people in the Chicago area. Because the pills came from different production plants and were sold in different drug stores around the Chicago area, police concluded that someone was tampering with the Tylenol on the store shelves. Panic ensued as Johnson & Johnson recalled the pills and merchants scrambled to remove the bottles to try and control the problem. Chicago police even took to the streets with loudspeakers to warn everyone. The panic factor was very high.
ATTENTION REALITY SPY STORY BUFFS

Published Summer 2014!

In the years just before WW II broke out in Europe, New York City (NYC) was home to a Nazi espionage group, known to history as the “Duquesne Spy Ring.” According to Spymuseum.com, it was “established in order to gather information that could be used in the event the United States entered the war—assigned to find holes in American military forces and preparedness before the United States entered the war and to find ways to destabilize the country and its morale.”

Enter naturalized US citizen William G. Sebold (1899 – 1970). In an FBI account, while in Germany in 1939 visiting his mother, Sebold was asked “by high-ranking members of the German Secret Service” to spy on America. Sebold received espionage training in Hamburg, but not before secretly visiting the American consulate in Cologne and telling officials there that he wanted to “cooperate with the FBI.”

Back in NYC, the FBI set up Sebold in an office rigged with cameras to see who would visit. It was in that location where 33 members of the Duquesne Spy Ring, including its leader, were discovered and eventually arrested.

This new book by Peter Duffy tells the story. Read the Kirkus review: https://www.kirkusreviews.com/book-reviews/peter-duffy/double-agent-first-hero/

Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), a joint and collaborative effort by the US Department of Homeland Security and the FBI, is another vehicle to detect terrorism, try to prevent action, and related criminal activity. The SAR and NSI are able to share information on a national level with state and local law enforcement partners.

Have You Obtained A TSA Pre-Approval for Domestic Travel?
Click on this link: TSA Pre✓™
Cute, friendly, and sporting very sensitive noses, Beagles are a critical component in the battle to keep harmful plant pests and foreign animal disease off US soil. According to the Customs and Border Protection (CBP) website, “detector dogs” have been manning our points of entry since 1984, when the US Drug Administration (USDA) instituted a “Beagle Brigade” program at Los Angeles International Airport (LAX). “Beagles and Beagle mixes are the preferred breed of dog at the airport because of their keen sense of smell, non-threatening size, high food drive, and gentle disposition with the public.”

They have a unique ability to discriminate and target a specific odor and, equally important, they can detect agricultural products, from bananas and fig trees to sausages and snails, much more quickly than a human inspector. “A trained agriculture dog can scan a piece of luggage in mere seconds,” claims the CBP. After making a discovery, they get a treat, of course.

The USDA transferred agricultural inspectors to the CBP in 2003, including roughly 75 canine teams. Today, there are more than 110 CBP Agriculture Canine teams providing screening at the border crossings, pre-clearance locations, air passenger terminals, cargo warehouses, and mail facilities that process international passengers and commodities.” Not all are beagles, however.

In 2000, Labrador Retrievers began working as agricultural detector dogs outside the “passenger environment.” All Beagles used by the CBP as agriculture detectors are either rescued from US shelters or obtained via “private donations” and must go through the Agriculture Specialist Canine Training with their human handlers at the USDA National Detector Dog Training Center in Georgia.

---

### Meet Kayla from Atlanta, Georgia

**Breed/Year Started**
Beagle/2010

**Favorite Odor**
Mango

**Life Before CBP**
Shelter in Rabun County, GA

**Specialization**
Agriculture Products

**Notable Seizures**
1 pound of cassava roots w/soil contaminated w/plant parasitic nematode

**Detection**

**Best Trick**
Begging for more treats

**Pet Peeve**
When other Beagles find contraband

---

Photos courtesy of the CBP
In honor of the 70th anniversary of the D-Day invasion, on June 6, 2014, the FBI celebrated a landmark that was home to one of the Bureau’s intelligence successes during World War II.

Overlooking Long Island Sound, it was at Benson House, from January 1942 until the end of the war in Europe in 1945, that FBI agents and radio technicians lived and worked undercover, secretly transmitting coded messages that the Nazis believed came from their own spies operating in New York. The Nazis believed their operatives were funneling significant details about US forces, munitions, and war preparations. But, in fact, the transmissions were controlled by the FBI—the Nazi spies were FBI double agents.

The Bureau’s work—known as Operation Ostrich—was central to the US counterintelligence operations throughout the war and was part of a larger effort by Allied Forces to deceive the enemy. That Allied Forces activity was identified as Operation Bodyguard.

Misleading Adolf Hitler’s intelligence services was integrated into the long preparation for the June 6, 1944 landing of 160,000 Allied troops in Normandy, France. Operatives set out to deceive the Nazi leader about the nature and location of the main Allied thrust so that he would be ill-prepared to meet the invasion. The key to Bodyguard’s success was the Allies’ control of a number of German spies and their ability to read coded German messages that confirmed the Nazis didn’t know their agents were compromised.

For the FBI, the initial purpose in participating in the counterintelligence effort was to learn about Nazi espionage—who was involved, how they worked, and what they wanted to know. Early on, intelligence from one double agent’s transmission indicated the Nazis were very interested in US experiments with atomic energy. This, in part, spurred US efforts to build the atomic bomb before the Nazis could.

The secretive work at Benson House proved even more valuable because that work allowed the United States to plant misleading information for Nazi officials—essentially controlling what the enemy knew about the US and its state of military readiness. In the case of Operation Bodyguard, it allowed America to help Allied efforts to protect the D-Day invasion plans.

The Ostrich information was often hard to come by. In those days, secrecy was paramount and cooperation was just

Continued on page 6

“In wartime, truth is so precious that she should always be attended by a bodyguard of lies.”
~ Winston Churchill

Source: FBI.gov
beginning between the FBI and overseas intelligence services, such as the British Secret Intelligence Service, now more commonly known as MI-6. But through the Bureau’s newly formed legal attaché office in London, the FBI began reviewing the British decrypts at MI-6 in January 1943. The bits of intelligence related to possible German espionage on US soil were passed to FBI Headquarters and then on to Bureau agents for action.

It helped the US, for example, in Argentina, where a network of secret Nazi radio stations had sprung up after being shut down in Brazil in 1942. With the help of Ostrich messages decoded both by the British and by cryptanalysts in the FBI Laboratory, the Bureau learned of the strong political influence and extensive intelligence activities of German agent Johannes Becker, mapped out the operation of his ring, disrupted its work throughout the war, and later shut it down completely in the summer of 1945.

Without Operation Ostrich, the FBI would not have been as successful in pinning down the extent of Nazi espionage in South America through the SIS. On a broader level, Ostrich intelligence enabled the Bureau to control the movements of its double agents and ensure they were successful in penetrating German intelligence. It was, in the end, one of the FBI’s most significant sources of intelligence in World War II.

Even after the fall of Germany in 1945, Nazi intelligence officials believed that the hundreds of messages sent by their spies in the US were real. The FBI’s efforts to contribute to the Allied “bodyguard of lies” were among the many Bureau intelligence efforts during the war and were surely some of the most significant.


This plaque was placed on Benson House on June 6, 2014, the 70th Anniversary of the D-Day invasion. The plaque commemorates the work accomplished at this pivotal place where counterintelligence activities led to one of the most successful plans devised by the FBI during World War II, tricking the Nazis to believe their intelligence sources were German agents.
News stories about continual espionage situations, stories that don’t make the “main” newspapers, online news, or any of the popular 24/7 news channels, exist in many other places of reference. The following are some MEDIA BITS for your reading pleasure:

* LIFE SENTENCES FOR SERIOUS CYBERATTACKS
The UK government stated it wants to hand out life sentences to anyone found guilty of a cyber attack that has a catastrophic effect, under plans announced in a recent speech by Queen Elizabeth II speech.
Any hackers that manage to carry out “cyber attacks which result in loss of life, serious illness or injury, serious damage to national security, or a significant risk thereof” would face the full life sentence, according to the serious crime bill proposed in that speech in June 2014.
As well as targeting cyberterrorists, the new offence in the proposed update to the Computer Misuse Act 1990 would also hand harsher sentences to those hackers carrying out industrial espionage, believed to be a growing menace affecting UK business.

* SOFTWARE THAT SEES EMPLOYEES, NOT OUTSIDERS, AS THE REAL THREAT
http://www.npr.org/blogs/alltechconsidered/2014/06/16/322580735/software-that-sees-employees-not-outsiders-as-the-real-threat
A growing number of companies are under pressure to protect sensitive data—and not just from hackers lurking outside the digital walls. They’re also looking to protect it from insiders—employees who may want to swipe information such as customer bank account numbers or electronic medical records.
A new breed of security software is hitting the market to help with insider threat detection. Lamar Pierce, a management professor at Washington University’s Olin Business School, has another concern. He’s seen managers misuse surveillance tools and effectively pick fights with employees who play a little fantasy football on the job.
Pierce says there’s an inherent problem with mission creep, where bosses ask the wrong questions: “Why don’t we start monitoring directly what people are doing during the afternoon? Why don’t we starting reading people’s emails to see if they say anything bad about the boss?”

* LEAKED DOCUMENTS REVEAL LAW ENFORCEMENT HACKING METHODS
Through the sourcing of a leaked documents cache from the Italian firm Hacking Team, members of the University of Toronto’s Citizen Lab have revealed the methods of law-enforcement hackers. While much of Snowden’s revelations concerned broad international surveillance, documents from Hacking Team reveal more specific methods such as the actual techniques for tapping phones and computers to operate as eavesdropping devices.
* INSIDER ATTACKS THWARTED BY AFGHANS


Camp Shorabak, Afghanistan—More than a year has passed since a Marine in Afghanistan was killed in a “green-on-blue” attack, but a pair of close calls in Helmand province this year at Afghan National Army training camps prove that insider attacks remain a high-profile threat to troops.

Marine advisers say, however, that while troops are forced to stay vigilant, improved cultural training has better-equipped them to recognize danger signs before they escalate.

Marine Corps Times previously reported that a member of the ANA had foiled a potential insider attack during a weapons class near Forward Operating Base Nolay in April, wrapping an armed fellow soldier in a bear hug after he allegedly announced that he planned to shoot an American. The paper has since learned of another incident earlier this year that was also thwarted by an Afghan soldier.

* IS ESTONIA’S RUSSIAN COUNTERINTELLIGENCE PROGRAM THE WORLD’S BEST?

http://intelnews.org/2014/06/05/01-1491/

Until not so long ago, the former Soviet Republic of Estonia was known as a playground for Russian intelligence. The tiny Baltic state, with a population of just under 1.4 million, a fourth of whom are ethnic Russians, struggled to build its security and intelligence infrastructure following its emergence from communism. Some of the country’s low points during that process include the infamous 2007 cyberattacks, which are believed to have been orchestrated by Moscow, and which kicked the entire country off the World Wide Web for over a week. A year later, authorities in Tallinn announced the arrest of Herman Simm, a senior official at the Estonian Ministry of Defense, who was apprehended along with his wife for spying on behalf of Russian intelligence for nearly 30 years.

Since that time, however, Tallinn has been able to transform its Russian counterintelligence program into something resembling the envy of the world, according to Foreign Affairs columnist Michael Weiss.

* HOW IRAN DUPED HIGH-RANKING US OFFICIALS WITH FAKE WEBSITE


Iran appears to be the hidden hand behind a three-year cyber-espionage campaign aimed at stealing information from leading high-ranking US military and diplomatic officials via an elaborate fake online news operation, according to a new report.

In spirit, if not daring, the fake news operation offers a whiff of e-payback for the CIA’s own fake movie-making gambit of 35 years ago, as dramatized in the movie “Argo,” in which US Embassy staff who evaded Iranian revolutionary hostage-takers was rescued.

Fake news stories, a fake media mogul who supposedly owned the news site they appeared on, his fake friends, and fake reporters who worked for him were all part of an extensive structure of fictitious personas, pictures, and messages strung across a host of social media sites including LinkedIn, Facebook, and Twitter.
IN CASE YOU MISSED SOME NEWS REPORTS...

* ISRAEL’S AGGRESSIVE SPYING IN THE U.S. MOSTLY HUSHED UP

http://www.newsweek.com/israels-aggressive-spying-us-mostly-hushed-250278

When White House national security advisor Susan Rice’s security detail cleared her Jerusalem hotel suite for bugs and intruders Tuesday night, they might’ve had in mind a surprise visitor to Vice President Al Gore’s room 16 years ago this week: a spy in an air duct.

According to a senior former U.S. intelligence operative, a Secret Service agent, who was enjoying a moment of solitude in Gore’s bathroom before the VP arrived, heard a metallic scraping sound. “The Secret Service had secured [Gore’s] room in advance and they all left except for one agent, who decided to take a long, slow time on the pot,” the operative recalled for Newsweek. “So the room was all quiet, he was just meditating on his toes, and he hears a noise in the vent. And he sees the vent clips being moved from the inside. And then he sees a guy starting to exit the vent into the room.”

Did the agent scramble for his gun? “No,” the former operative said with a chuckle. “He kind of coughed and the guy went back into the vents.”

* TONY ABBOTT DEFENDS ROLE OF FIVE EYES INTELLIGENCE ALLIANCE


Tony Abbott defended the role of the Five Eyes Intelligence-Sharing Alliance while on tour in North America, saying it should never apologise (sic) for “doing what’s necessary,” confirming he is hoping to meet Rupert Murdoch in New York.

The Australian leader arrived in Canada to meet the country’s Prime Minister, Stephen Harper, a fellow conservative. Canada is part of the Five Eyes Alliance along with Australia, England, New Zealand and the US. Abbott declared the US the “heavy lifter” of the group.

Revelations from the whistleblower Edward Snowden have raised controversy about the Alliance’s activities. “Obviously we have to be intelligent about our intelligence. I mean that goes without saying, but the important thing is not to be deterred from doing what is necessary to protect our citizens, our interests and our values, and what is sometimes forgotten about the work of the Five Eyes is that it’s not just for the benefit of those five countries but it is ultimately for the benefit of the wider world,” Abbott told reporters in Ottawa when asked if Five Eyes should assess its spying practices.

* FACE SCAN SYSTEM TO THWART TERRORISTS


A new "biometric" identification system designed to thwart the use of false passports by terrorists such as Khaled Sharrouf will be introduced to airports around the country.

The rollout of the $158 million "eGate" departure-gate scanning system adds to recent announcements about the establishment of airport terrorism units.

Sharrouf, a convicted terrorist, is notorious for leaving Australia on his brother’s passport, then becoming an active participant in Islamic State’s incursions in Syria and Iraq. He made headlines when pictures of his son were published holding the severed head of a Syrian soldier.

Minister for Immigration and Border Protection Scott Morrison said the electronic departure gates would be rolled out from mid-next year.
**In Case You Missed Some News Reports...**

* **RICIN TOXIN VACCINE SHOWS PROMISE IN A NON-HUMAN PRIMATE STUDY**  
  [Link](http://www.homelandsecuritynewswire.com/dr20140908-ricin-toxin-vaccine-shows-promise-in-a-nonhuman-primate-study)  
  Ricin toxin is a plant toxin thought to be a bioterror threat because of its stability and high potency as well as the large worldwide reservoir created as a by-product of castor oil production. As a poison, ricin is so potent that the U.S. Centers for Disease Control (CDC) estimates the lethal dose in humans is about the size of a grain of salt. There are currently no effective means to prevent the effects of ricin poisoning. Soligenix, Inc., a clinical stage biopharmaceutical company developing several biodefense vaccines and therapeutics, announced last week promising preliminary results from a preclinical study with its ricin toxin vaccine RiVax, in a non-human primate (NHP) lethal aerosol exposure model.

* **CAPTURED DOCUMENTS REVEAL IS’S INTEREST IN ACQUIRING BIOTERROR WEAPONS**  
  [Link](http://www.homelandsecuritynewswire.com/dr20140903-captured-documents-reveal-is-s-interest-in-acquiring-bioterror-weapons)  
  Terrorist organizations have been trying to acquire or build biological weapons of mass destruction, and now, with the growing threat of the Islamic State (IS), analysts are concerned that the Islamist group may gain access to bio-labs in Syria or Iraq. A laptop belonging to a Tunisian who joined ISIS was recently found in Syria, contained documents about how to build and use biological weapons.

* **FROM THE ARCHIVES**  
  [Link](http://www.archives.gov/iwg/research-papers/red-orchestra-irr-file.html)  
  The Red Orchestra is perhaps one of the best known espionage cases of the Second World War.¹ The U.S. Army’s Investigative Records Repository (IRR) file on the Soviet espionage network, being released under the Nazi War Crimes Disclosure Act, contains documents related to an investigation of the Red Orchestra case during the early postwar period. It is clear from the contents of the file that Allied intelligence officers were interested, not in possible Gestapo misdeeds (use of torture) in eradicating the Red Orchestra, but rather in what information about Soviet military intelligence practices might be gleaned from German files and from interrogating those Germans involved with the case.

One of the most interesting documents in the file is a report dated 11 February 1952. The report concerns a meeting between a special agent of the 66th CIC Detachment and Dr. Manfred Roeder, formerly the Judge Advocate of the German Air Force (Luftwaffe) who served as the assistant prosecutor in the espionage case involving Red Orchestra agents. The meeting, which took place in Hannover, Germany, was arranged through Graf Wolf von Westarp, a leading figure in the Sozialistische Reichspartei (Socialist Reichs Party, or SRP), a postwar German rightist party. At this time, the CIC was actively pursuing leads concerning the Red Orchestra case. According to rumors, some “eight crates of documents” concerning the case had been hidden by German intelligence personnel in the Lüneburger Heide shortly after the war. Thus, the meeting with Roeder was intended to elicit information necessary to allow CIC agents to locate and exploit the Red Orchestra records.

---

**Reward for Information**

FBI Special Agent James Daugherty has a dozen years of experience investigating spies, and in almost all of the cases he has worked, the subjects’ families, friends, or colleagues had concerns but failed to report them to authorities. “The FBI needs the public’s help to fight the insider threat,” Daugherty said, “and we are willing to pay for that help.”

Individuals who provide information leading to the arrest and conviction of a spy—or to the prevention of espionage—are eligible for a $500,000 reward. Contact your local FBI office or submit an anonymous tip online if you suspect and want to report suspicious activities of family, friends, or co-workers.
You may have read the book about Edward Snowden, written by The Guardian reporter Luke Harding, titled *The Snowden Files: The Inside Story of the Worlds’ Most Wanted Man*. But did you know there’s a film in the works? The movie will be directed by Oliver Stone, based on Harding’s book as well as on a novel by Snowden’s Russian lawyer, Anatoly Kucherena.

Harding’s book has been hailed by The New York Times as a “fast-paced, almost novelistic narrative that is part bildungsroman and part cinematic thriller.” Kucherena’s book, according to one account, is a thinly veiled fictional tale of his American client’s odyssey since spilling NSA secrets. The title is *The Time of the Octopus*.

It will be interesting to see how Mr. Stone, who bought the rights to both books, spins the story to be told in the film and who will play the hero/villain, depending on your POV. Filming is expected to begin by the end of the year.

---

**Homeland Security and Private Sector Business:**

Corporations' Role in Critical Infrastructure Protection,

SECOND EDITION

BY

Elsa Lee

Noted Counterintelligence Expert

Businesses, Universities, & Individual Readers ALL find this book to be extremely informative.

Useful as a teaching tool and curriculum starter,
as well as a textbook for seminars and classes,

it has been read by more than 100,000!

*A review published by The Berkeley Electronic Press for the first edition in 2010 said:*

“Overall, the book offers a new look at homeland security and critical infrastructure protection based on a different definition of threats and protection measures. Current threats are different in terms of their nature and their potential impacts. Education and training of human resources and management seems to be the most effective approach in protecting critical infrastructure. Cooperation among industries, government, and the private sector is also important in homeland security.”

Available after December 15, 2014, on Amazon.com, Kindle.com, and online at CRC Press
How much do you know about the world of security? What questions will stump your knowledge? Answer as many of the following questions as you possibly can and send them to info@advantagesci.com to receive all the correct answers in a return email. The first five (5) responders will receive an online gift certificate.

1. A person who willingly commits espionage is a __________.
2. To warn or make aware is to __________.
3. Firearms and explosives are examples of what type of items _____________.
4. Written documents that remind us of security responsibilities are _____________.
5. A technique to secure the services of someone, to engage that person, or hire them is best described as _____________.
6. The abbreviation for a business trip in support of the mission is _________.
7. Another word for important; essential is _____________.
8. The abbreviation for a security mechanism that uses a set of letters or number on a lockable container is a _____________.
9. The possibility or chance of loss is to _____________.
10. A type of classified information that will cause extremely grave damage to national security if disclosed is known as _____________.
11. ____________ are known as “our most vital resource.”
12. When overseas, report security concerns to _____________.
13. A signal with loud screeching noises and flashing lights is an _____________.
14. A type of briefing required when you no longer plan to work for NSA/CSS or other national security agencies is described by the word _____________.
15. Security incidents involving computers are reported to the _____________.
16. Material above the Top Secret level must be stored in a container called a _____________.
17. Information that pertains to sources and methods is known as _____________.
18. The practice of spying or using spies to obtain information about the plans and activities of a foreign government is _____________.
19. This is usually the main motivator for spying. _____________.
20. An infection to your computer is a _____________.
21. In order to protect your computer from unauthorized access you must create a _____________.
22. This is installed to protect a perimeter. _____________.
23. To be granted a TS/SCI clearance, an individual must pass a _____________.
24. Good security practices are illustrated by hanging these on walls. _____________.
25. A four-digit number to be used with your badge is known as your _____________.

was associated with agriculture, and agriculture-related industries contributed to 4.8% share of the US GDP.

Let’s look at corn. *America runs on corn.* We each consume 25 pounds of corn annually, and it’s in everything—from edibles, such as breakfast cereal, snacks, and sodas, to non-edibles such as paint, shoe polish, and candles. We put corn in our cars. We lead the world in corn production—95.4 million acres were planted in the US in 2013.² Imagine if our corn harvest was completely destroyed for a single year, or worse, for several years until science could find a way to safely and effectively destroy whatever had infiltrated the crop of US corn?

The Department of Homeland Security Customs and Border Protection (CBP) understands that our agriculture is a critical, hard-to-protect component of our infrastructure, and works diligently to prevent the introduction of destructive pests and diseases through an aggressive agricultural inspection program. Inspectors look for what the CBP refers to as “actionable pests.”

According to the CBP website, “...if introduced into the United States, actionable pests have the potential to have significant economic impact on American agriculture and natural resources because they are either non-existent in the US or currently have very limited distribution in the country.” Even the humble apple in your backpack is denied entry. As one CBP official noted, “Something as simple as an apple could carry the larva of a Mediterranean fruit fly, which, if it got loose in our citrus crops... could cost billions of dollars.”

In 2013, approximately 160,000 potentially dangerous pests were intercepted by CBP agriculture specialists at 328 land, air, and seaport points of entry. Most arrived with confiscated plant materials, meat, and animal by-products.³ CBP agricultural inspectors recently discovered two “actionable pests” in the DC Metro area:

**April 2014**—Dulles International: Inspectors intercepted a Popular Hawk Moth, arriving in a shipment of cut flowers originally grown in Uganda. USDA analysis found that the moth “could pose a significant agriculture threat because they are known to feed on a wide variety of trees, such as poplar, aspen, willow, alder, birch, elm, oak, and ash.”

**May 2014**—Port of Baltimore: Inspectors discovered a type of moth in a shipment of bulk organic soybeans from China known to feed on seeds and grains, posing a distinct threat to farmers.

Animal diseases can be imported as well. Consider the highly contagious Foot and Mouth Disease (FMD) (mistakenly named “Hoof and Mouth Disease” for years). The FMD virus causes illness in cows, pigs, sheep, goats, deer, and other animals with hooves. FMD can spread rapidly and, while the US eradicated the disease in 1929, it is currently found in parts of Africa, Asia, Europe, and South America. Many animals and animal by-products from these areas are subject to import restrictions or are completely prohibited from entering the US.

<table>
<thead>
<tr>
<th>2001 FMD Outbreak in the UK at a Glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>2,030 confirmed cases spread across the country</td>
</tr>
<tr>
<td>6 million animals culled/4 of the 6 million as part of disease control</td>
</tr>
<tr>
<td>£3.1 billion loss to agriculture and the food chain industries</td>
</tr>
<tr>
<td>£2.5 billion compensation paid by the government to farmers</td>
</tr>
</tbody>
</table>

Source: Department for Environment, Food, and Rural Affairs (defra.gov.uk)

In 2001, the United Kingdom (UK) experienced its worst outbreak of FMD, resulting in millions of slaughtered animals and staggering economic losses—most especially in the agricultural sector, but also in rural tourism and industries dependent on livestock production. The disease spread quickly, carried on the wind to neighboring farms, via the movement of animals, and tracked by people and vehicles. It took a full year to control the disease. Although how FMD was introduced into the country was never clearly ascertained, investigators believed the virus arrived in infected or contaminated imported meat or meat by-products consumed by pigs on the farm where the FMD outbreak was discovered. Imagine the impact such a virulent disease would have in the US if deliberately introduced. The way American animal usage for food is concentrated in specific locations for production makes our livestock extremely vulnerable to infiltration by any disease or tampering with their food.

We’ve been fortunate so far. Our food animals and crops have not been targeted, and we might conclude that the CBP/USDA inspection program is working. It’s also possible that terrorists have simply not yet agreed on a plan to deliver agro-devastation to our doorstep. And while we can hope to control what enters our country at the borders, we have less control over what a homegrown, technically skilled terrorist might cook up in a New York City apartment, and, then, deliver to our fields and food production facilities.

A terrorist does not have to explode airplanes into skyscrapers to send a message. Creating fear and panic on a smaller scale is an effective message carrier too. Our food supply is vulnerable and there is ample opportunity for maliciousness—at every step between the farm and the fork. But at least we have the borders covered and we want to thank everyone at the CBP for working diligently to help protect our food supply.

CREDIT CARD SKIMMERS ON GAS PUMPS

Most people who live in the US (other than New Jersey and Oregon residents) pump their own gas at the pump and use their credit or debit card to pay for the transaction. Thieves are now using their own devices to skim information from those credit/debit cards and the magnetic security strip. By tampering with the pump’s card reader, they are installing a “dummy” card slot on top of the card slot installed at the factory or a duplicate key pad over the real key pad, downloading the information onto a hidden device the thieves have installed inside the computer of the gas pump, retrieving the data periodically. Unfortunately, the keys that allow access to these areas on gas pumps are “universal” and easily used on any pump, making tampering a fairly easy task.

If possible, pay for your gas with cash and avoid being a victim of gas pump credit card skimming.

ADVANTAGE SCI PRODUCTS, SERVICES, AND TRAINING

Advantage SCI offers services supporting the counterintelligence (CI) needs of the cleared defense contractor community, private business, government, utilities, and municipalities with requirements to protect classified information, trade secrets, intellectual property, and other privileged information. Services include:

- Vulnerability Assessments
- Threat Briefings/Foreign Travel Briefings/Debriefings
- Counterintelligence Awareness Training/Insider Threat Training
- TSCM Services in classified or unclassified spaces
- Facility Security Officer (FSO) In a Box
- Active Shooter Seminar/Smartphone Risks & Vulnerabilities
- Consult With a CI Professional
- Foreign Travel Briefings and Debriefings
- Intelligence Analysis/Intelligence Analysts
- Plans, SOPs, Regulatory-related materials
- Workplace Violence Prevention and Response
- Other matters related to improving CI-related posture

Advantage SCI’s Vision

“Educate America’s 300 million people and business leaders on prevention, detection, and response to 21st century threats.”

Advantage SCI: SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS (SDVOSB), SMALL BUSINESS ENTITY (SBE), MINORITY-OWNED BUSINESS ENTITY (MBE), SMALL DISADVANTAGED BUSINESS ENTITY (SDB), WOMAN-OWNED BUSINESS ENTITY (WBE)

Visit our website: http://advantagesci.com