UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA	*	
	*	
v.	*	
	*	**MAGISTRATE NO. BPG-16-2254**
HAROLD T. MARTIN, III,	*	
	*	
	*	
Defendant	*	
	*	
	*******	

GOVERNMENT'S RESPONSE TO DEFENDANT'S MOTION FOR A DETENTION HEARING

For over two decades, the Defendant, Harold T. Martin, III, was entrusted to work at multiple government agencies dealing with highly classified information, including the National Security Agency ("NSA"). Throughout his government assignments, the Defendant violated that trust by engaging in wholesale theft of classified government documents and property—a course of felonious conduct that is breathtaking in its longevity and scale. The Defendant's decades of criminal behavior were in flagrant violation of his many promises and oaths, as well as the law. The case against the Defendant thus far is overwhelming, and the investigation is ongoing. The Defendant knows, and, if no longer detained may have access to, a substantial amount of highly classified information, which he has flagrantly mishandled and could easily disseminate to others. The government intends to file additional serious felony charges as described herein. After betraying the most important trust the United States can grant, the Defendant presents a high risk of flight, a risk to the nation, and to the physical safety of others. After twenty years of violating the nation's trust and its laws, the Defendant now asks the Court to place similar trust in him to remain in the United States and abide by any conditions of release set by the Court. The Court should deny that request.

I. PROCEDURAL POSTURE

On August 27, 2016, the Defendant was arrested during the execution of several search warrants, one of which was for his residence. On August 29, 2016, the Defendant was charged by criminal complaint with Theft of Government Property, in violation of Title 18, United States Code, Section 641, and Unauthorized Removal or Retention of Classified Documents or Materials by Government Employee or Contractor, in violation of Title 18, United States Code, Section 1924. The complaint and supporting affidavit were filed under seal, pursuant to Court order.

On August 29, 2016, the Court held an initial appearance on the complaint. The courtroom was closed at the time of the hearing, on motion of the government and with the consent of the Defendant. At the initial appearance, the Court appointed the office of the Federal Public Defender to represent the defendant. The government moved for detention, and the Defendant consented to detention without prejudice to seeking a detention hearing at a later date.

On September 8, 2016, the Defendant submitted a written waiver of preliminary hearing. On September 13, 2016, the government filed a consent motion to extend the period within which an indictment or information must be filed. The same day, the Court entered an order extending the period within which an indictment or information must be filed to March 1, 2017.

On October 5, 2016, the government moved to unseal the case, and the Court granted the government's motion. On October 17, 2016, the Defendant filed a motion seeking a detention hearing. A detention hearing is currently scheduled for 2:15 p.m. on Friday, October 21, 2016, before United States Magistrate Judge A. David Copperthite.

As set forth below, the government seeks the Defendant's continued pretrial detention based upon the grave danger his release would pose to the community and the serious risk that he may fail to appear as required.

II. RELEASE OF THE DEFENDANT WOULD POSE A DANGER TO THE NATION'S SECURITY

At the hearing, the government will proffer evidence demonstrating that each of the factors to be considered under the Bail Reform Act supports detention of the Defendant pending trial in this case. The evidence will make clear that the nature and circumstances of the offenses, the history and characteristics of the Defendant, and the overwhelming weight of the evidence all support detention of the Defendant pending trial. Most important, however, is the grave and severe danger that pretrial release of the Defendant would pose to the national security of the United States.

A. The Offenses are Extremely Serious and Merit Pretrial Detention

The evidence provides ample probable cause to believe that the Defendant has committed extremely serious offenses against the United States and should be detained. *See* 18 U.S.C. § 3142(g)(1). The pending charges are very serious. During execution of the search warrants, investigators seized thousands of pages of documents and dozens of computers and other digital storage devices and media containing, conservatively, fifty terabytes of information. The seized hard copy documents that were seized from various locations during the search comprise six full bankers' boxes worth of documents. Some of the documents are marked "Unclassified/For Official Use Only," and many are marked "Secret" and "Top Secret." Many of the documents marked "Secret" and "Top Secret," also bear special handling caveats. The information stolen by the Defendant also appears to include the personal information of government employees. The seized digital media included computers, external hard drives, optical discs and a number of USB thumb drives.

The Defendant stole from the government and hid at his residence and in his vehicle a vast

amount of irreplaceable classified information. His thefts involved classified government materials that were dated from 1996 through 2016, spanning two decades' worth of extremely sensitive information. For example, the search of the Defendant's car revealed a printed email chain marked as "Top Secret" and containing highly sensitive information. The document appears to have been printed by the Defendant from an official government account. On the back of the document are handwritten notes describing the NSA's classified computer infrastructure and detailed descriptions of classified technical operations. The handwritten notes also include descriptions of the most basic concepts associated with classified operations, as if the notes were intended for an audience outside of the Intelligence Community unfamiliar with the details of its operations.

Among the many other classified documents found in the Defendant's possession was a document marked as "Top Secret/Sensitive Compartmented Information" ("TS/SCI") regarding specific operational plans against a known enemy of the United States and its allies. In addition to the classification markings, the top of the document reads "THIS CONOP CONTAINS INFORMATION CONCERNING EXTREMELY SENSITIVE U.S. PLANNING AND OPERATIONS THAT WILL BE DISCUSSED AND DISSEMINATED ONLY ON AN ABSOLUTE NEED TO KNOW BASIS. EXTREME OPSEC PRECAUTIONS MUST BE TAKEN." The Defendant was not directly involved in this operation and had no need to know about its specifics or to possess this document.

A conservative estimate of the volume of the digital information seized from the Defendant is approximately 50,000 gigabytes.[1] This information must be fully reviewed by appropriate authorities to determine its source and classification level, as well as the extent to which it

[1] A gigabyte (GB) is sufficient storage space for approximately 10,000 pages of documents containing images and text.

constitutes "national defense information." The investigation into the Defendant's unlawful activities is ongoing, including review of the stolen materials by appropriate authorities. The government anticipates that much of this material will be determined to be national defense information that the government goes to great expense to protect.

The improper retention and transmission of national defense information is prohibited under the Espionage Act. *See, e.g.,* 18 U.S.C. § 793 (Gathering, Transmitting or Losing Defense Information). Information about sources and methods of the Intelligence Community, such as the information in the documents described above, and in the criminal complaint, is classic national defense information. *See Gorin v. United States*, 312 U.S. 19, 28 (1941) (information relating to the national defense is "a generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness."). In this case, when an indictment or information is filed, the government anticipates that the charges will include violations of the Espionage Act, an offense that carries significantly higher statutory penalties and advisory guideline ranges than the charges listed in the complaint.

Congress has recognized the seriousness of compromising the security of classified information through substantial criminal penalties. *See* 18 U.S.C. §§ 641, 793. Moreover, the Defendant's alleged crimes, and the anticipated additional charges, are extremely serious within the meaning of the Bail Reform Act. The Defendant's crimes reflect a willingness to routinely betray the trust of the nation, and there is no reason to believe that, if released, the Defendant will have any greater regard for any trust placed in him by the Court.

B. <u>The Evidence of the Defendant's Guilt is Overwhelming</u>

The weight of the evidence against the Defendant is overwhelming. *See*

18 U.S.C. § 3142(g)(2). The Defendant was in possession of an astonishing quantity of marked classified documents which he was not entitled to possess, including many marked TS/SCI, that appear to contain national defense information. Many of the marked documents were lying openly in his home office or stored in the backseat and trunk of his vehicle.

In his non-custodial interview, the Defendant initially lied to investigators and denied taking classified information from his work assignments, notwithstanding the documents left lying about in his vehicle and home. When confronted with specific marked documents he had stolen, only then did the Defendant begin to admit that: (1) he had taken documents and digital files that he knew were classified from his work assignment to his residence and vehicle, and (2) he knew such actions were unauthorized and wrong. He also admitted that he had committed these crimes regularly over many years. If the Defendant had not been arrested, it is clear that he would have kept these classified materials to use as he saw fit.

The Defendant had access to classified information, including Top Secret information, beginning in 1996. His access to classified information began during his service in the U.S. Naval Reserves, and continued as he worked for seven different private government contracting companies. Access to classified information was critical to the Defendant's employment in his field. He worked on highly classified, specialized projects and was entrusted with access to government computer systems, programs and information.

Over his many years holding a Top Secret security clearance, the Defendant had been trained on the proper handling and storage of classified materials. He signed a number of Non-Disclosure Agreements over two decades that reiterated the need to handle classified information appropriately, including documents that listed the potential criminal penalties for failing to do so.

One of the many trainings on protection of national security and classification included the following information:

> At any given moment, there are numerous countries spying against the United States—from our most dangerous enemies to our closest allies. They want our information. Our technology. Our deepest secrets. And while many of these threats come from the outside, perhaps the greatest security concern facing the nation today comes from within our most trusted circles.
>
> This concern is often, and correctly called . . . The Insider Threat. Millions of people are trusted with America's most important secrets. Vetted personnel who've made promises to protect this information at all costs. Millions of cleared people—but it takes just one person to undo it all. To waste years of research . . . to squander millions of dollars in technological innovation . . . to put thousands of people in harm's way.
>
> Our information is valuable and the economics of espionage are simple. Why spend billions developing a military program when you can spend a fraction of the cost to simply steal it? But beyond money, imagine how the United States' critical information could allow adversaries to exploit our weaknesses—discovering holes in our defenses . . . and providing those who would do us harm an increased advantage to steal the liberty and lives of our fellow citizens and allies.
>
> Whether intentional or not, when someone fails to safeguard critical information or protect our computer networks from the ever-present threat, the impact can be felt for decades. It's your duty to protect the information you have access to. And if you believe someone else is placing that information—or themselves—in danger, it's your responsibility to say something. It only takes one person to betray a nation . . . or to save it.

As a trusted insider, the Defendant was able to defeat myriad, expensive controls placed on that information. The evidence is overwhelming that the Defendant abused this trust and chose to repeatedly violate his agreements, his oaths and the law—and to retain extremely sensitive government information to use however he wished.

C. The Defendant's Technical Knowledge and History of Criminal Behavior Warrant Pretrial Detention

The Defendant's history and characteristics also demonstrate that he should be detained. *See* 18 U.S.C. § 3142(g)(3). The Defendant has obtained advanced educational degrees and has taken extensive government training courses on computer security, including in the areas of encryption and secure communications. He has attended a number of prominent computer hacking conferences. The Defendant was enrolled in a Ph.D. program in information security management at the time of his arrest, and was engaged in research for his doctoral dissertation. His doctoral studies were in the same general subject area in which he worked as a private contractor assigned to the government.

Examination of the digital media seized from the Defendant indicates extensive use of sophisticated encryption, anonymization, and virtual machine technologies. There is evidence that he has remote data storage accounts and has engaged in encrypted communications. The Defendant also had encrypted communication and cloud storage apps installed on his mobile device. The Defendant has the knowledge and training to house some or all of the stolen digital information in cyberspace, where he could easily access or transfer it, were he to have access to the internet. The Defendant was in possession of a sophisticated software tool which runs without being installed on a computer and provides anonymous internet access, leaving no digital footprint on the machine. The Defendant's internet activity also suggests that he was attempting to locate anonymous internet access and to run operating systems on his machines that would not leave any forensic evidence of his computer activities. In July 2016 he watched a video about how individuals who attempt to remain anonymous on the internet are caught by authorities. He has a demonstrated ability to conceal his online communications and his access to the internet.

D. Pretrial Release of the Defendant Poses a Grave Danger to the Nation

Most importantly, the nature and severity of the danger that release of the Defendant would pose to the community can only be mitigated by pretrial detention. *See* 18 U.S.C. § 3142(e)(1) and (g)(4). In late July 2016, the Defendant traveled to Connecticut to purchase a "Detective Special" police-package Chevrolet Caprice. During execution of the search warrants, law enforcement officers recovered ten firearms, including an AR-style tactical rifle and a pistol-grip shotgun with a flash suppressor. Only two of his firearms were registered, although three others may have required registration depending on their date of purchase. The Defendant's wife was very upset to learn about the Defendant's arsenal, as she had only been aware of the Defendant possessing one or two of the firearms which were found in the home. In addition, a loaded handgun was found in a case lying on the rear driver's side floorboard of the Caprice, in apparent violation of Maryland law. If the Defendant stole this classified material for his own edification, as he has claimed, there would be no reason to keep some of it in his car, and arm himself as though he were trafficking in dangerous contraband. Prior to the Defendant's arrest, his wife asked law enforcement officers to remove the firearms from the home because she was afraid that he would use them to kill himself if he "thought it was all over." With her consent, all of the weapons were taken into the custody of the FBI.

The fact that digital and hard copy materials containing highly classified information were found in the Defendant's vehicle demonstrates that the materials were being transported and were available to anyone who may have gained access to his vehicle. The Defendant admitted that he regularly was transporting this material in his vehicle. The Defendant did not have an enclosed garage, and his vehicle was routinely parked in the driveway of his home, including when the

search warrants were executed.

As digital technology has proliferated, extremely small devices can be used to store or access digital information. Currently, the Defendant has no access to digital devices or unmonitored communications (except for communications with counsel). If he is released, he will have the ability to access and transmit any stolen classified information he may still have hidden or stored online. As a practical matter, should he be released, there is no way to prevent him from obtaining access to an internet-enabled device or from contacting another individual willing to assist him. Any order from this Court prohibiting this conduct could only be enforced after it is violated, and our nation's security has already been irrevocably compromised.

As a result of the extensive publicity this case has received, it is readily apparent to every foreign counterintelligence professional and nongovernmental actor that the Defendant has access to highly classified information, whether in his head, in still-hidden physical locations, or stored in cyberspace—and he has demonstrated absolutely no interest in protecting it. This makes the Defendant a prime target, and his release would seriously endanger the safety of the country and potentially even the Defendant himself.

In a review of the digital information seized from the Defendant, the government found a letter, apparently created in 2007, which was addressed to government employees with whom he worked, and signed "Hal." In the letter, the Defendant refers to his co-workers as "clowns" and criticizes the government's digital security measures:

> Well, for one thing, I've seen pretty much all your tech secrets wrt [sic] regard to compusec [computer security]. Thanks. You made me a much better infosec [information security] practitioner. In exchange, well, I gave you my time, and you failed to allow me to help you . . .
>
> You are missing most of the basics in security practice, while

> thinking you are the best. It's the bread and butter stuff that will trip you up. Trust me on this one. Seen it. . . .
>
> Dudes/Dudettes, I can't make this any plainer . . . Listen up . . . 'They' are inside the perimeter. . .
>
> I'll leave you with this: if you don't get obnoxious, obvious, and detrimental to my future, then I will not bring you 'into the light', as it were. If you do, well, remember that you did it to yourselves.

The antipathy demonstrated in this letter raises grave concerns about the Defendant's intentions and potential actions should he be released.

III. THE DEFENDANT POSES A SUBSTANTIAL RISK OF FLIGHT

The Defendant's behavior and characteristics also demonstrate that he is a significant flight risk. His incentive to escape the jurisdiction of this Court is in no way substantially limited by his apparent lack of a valid United States passport. Given the nature of his offenses and knowledge of national secrets, he presents tremendous value to any foreign power that may wish to shelter him within or outside of the United States. Should the Defendant flee to the "protection" of a foreign power, there is no guarantee that he would not ultimately come to harm. The severity of the potential penalties the Defendant faces, and will probably face should additional charges be filed, provides further incentive to flee the country and never return, or to seek refuge with a foreign government willing to shield him from facing justice in this Court in exchange for access to information that he knows or possesses. The Defendant has also communicated online with others in languages other than English, including in Russian, and in June 2016 downloaded information regarding the Russian language as well as other foreign languages.

The Defendant is the subject of an ongoing investigation, and the government intends to file additional charges against him prior to the expiration of the Speedy Trial Act deadline.

His wife indicated that he had previously told her that he would take his own life "if he thought if it was all over." The Defendant has lost his security clearance and his career, and is facing the loss of his freedom. He appears to have nothing left to lose, and every reason to attempt to evade the criminal consequences of his actions.

IV. CONCLUSION

The evidence demonstrates that the Defendant poses a danger to the community and to the national security of the United States, and is a substantial risk of flight. At this stage in the proceedings, no condition or combination of conditions will reasonably assure either the appearance of defendant at trial or the safety of the community and the nation. The Defendant should be ordered detained pending trial in this case.

Respectfully submitted,

Rod J. Rosenstein
United States Attorney

By: /s/

Zachary A. Myers
Assistant United States Attorney
36 South Charles Street, Fourth Floor
Baltimore, Maryland 21201
(410) 209-4800

By: /s/

David Aaron
Trial Attorney
U.S. Department of Justice, National Security Division
950 Pennsylvania Ave NW
(202) 307-5190