A.E.
2/3/17

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA	*	**CRIMINAL NO.** MJG17-069
v.	*	
HAROLD T. MARTIN III,	*	**(Willful Retention of National Defense Information, 18 U.S.C. § 793(e); Forfeiture 18 U.S.C. § 981)**
Defendant.	*	
	*	
	*	
	*	
	*******	

INDICTMENT

COUNTS ONE THROUGH TWENTY
(Willful Retention of National Defense Information)

The Grand Jury for the District of Maryland charges that:

At all times material to this Indictment:

General Allegations

The Defendant

1. Defendant **Harold T. Martin III ("MARTIN")**, now age 52, was a resident of Glen Burnie, Anne Arundel County, Maryland.

2. Beginning in or about December 1993, and continuing through on or about August 27, 2016, **MARTIN** was employed as a private contractor, assigned to work at a number of government agencies. In connection with his employment, **MARTIN** held various security clearances and had access to national defense and classified information.

Classified Information

3. Pursuant to Executive Order 12958 signed on April 17, 1995, as amended by Executive Order 13292 on March 25, 2003, and Executive Order 13526 on December 29, 2009, national security information was classified as "TOP SECRET," "SECRET," or

"CONFIDENTIAL." National security information was information owned by, produced by, produced for, and under the control of the United States government that was classified as follows:

a. Information was classified as TOP SECRET if the unauthorized disclosure of that information reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority was able to identify and describe.

b. Information was classified as SECRET if the unauthorized disclosure of that information reasonably could be expected to cause serious damage to the national security that the original classification authority was able to identify and describe.

c. Information was classified as CONFIDENTIAL if the unauthorized disclosure of that information reasonably could be expected to cause damage to the national security that the original classification authority is able to identify and describe.

4. Access to national security information classified at any level could be further restricted through compartmentation in Sensitive Compartmented Information (SCI) categories. Only individuals with the appropriate security clearance and additional SCI access(es) could have access to such classified national security information.

5. Classified information, including SCI, was marked according to its classification and applicable SCI compartments, following standard formats for different types of media, including headers and footers stating the highest classification level and SCI compartments of information a document contained and individual classifications markings for each paragraph.

6. Information classified at any level could only be accessed by persons determined by an appropriate United States government official to be eligible for access to classified information, who had signed an approved non-disclosure agreement, who received a security clearance, and who had a need to know the classified information. Classified information could only be stored in an approved facility and container.

Relevant Government Agencies

7. The U.S. Intelligence Community (USIC) consisted of U.S. executive branch agencies and organizations that worked separately and together to conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States.

8. The U.S. Department of Defense (DoD) was a U.S. executive branch agency, the mission of which was to provide the military forces needed to deter war and to protect the security of the United States.

9. The National Security Agency (NSA) was a U.S. government intelligence agency with various offices and facilities, and was a component of the USIC and DoD. NSA's primary facility and headquarters were at Fort Meade in the District of Maryland. NSA was responsible for, among other things, collecting, processing, and disseminating intelligence derived from intercepted foreign communications to U.S. policy-makers and military forces; protecting secure government systems that handle classified information and were otherwise critical to military and intelligence agencies, and Computer Network Operations (CNO), which involves operations and intelligence collection to gather data from target or foreign automated information systems or networks and actions taken to prevent, detect, and respond to unauthorized activity within DoD information systems and computer networks, for the United States and its allies.

10. United States Cyber Command (USCYBERCOM) was a U.S. military command and a component of DoD. USCYBERCOM's primary facility and headquarters were at Fort Meade in the District of Maryland. USCYBERCOM was responsible for, among other things, planning, coordinating, integrating, synchronizing, and conducting activities to direct the operations and defense of specified DoD information networks, and conducting full spectrum

military cyberspace operations to ensure freedom of action in cyberspace for the United States and its allies, and deny the same to the adversaries of the United States.

11. The National Reconnaissance Office (NRO) was a U.S. government intelligence agency with various offices and facilities, and was a component of the USIC and DoD. NRO's primary facility and headquarters were in Chantilly, Virginia. NRO was responsible for research and development, acquisition, launch, deployment, and operation of overhead systems and related data processing facilities to collect intelligence and information to support national and departmental missions and other United States government needs, including, among other things, the collection of signals and imagery data used to inform U.S. policy-makers and military forces on the strategic and tactical intentions and capabilities of the adversaries of the United States.

12. The Central Intelligence Agency (CIA) was a U.S. government intelligence agency with various offices and facilities, and was a component of the USIC. CIA's primary facility and headquarters were in northern Virginia. CIA was responsible for, among other things, collecting (including through clandestine means), producing and disseminating foreign intelligence and counterintelligence used to inform U.S. policy-makers; conducting counterintelligence activities; conducting administrative and technical support activities; conducting covert action activities approved by the President; and conducting foreign liaison relationships with intelligence and security services of foreign governments.

MARTIN's Access to National Defense and Classified Information

13. From in or about July 1988 through in or about July 1992, **MARTIN** served on active duty in the United States Navy. **MARTIN** held a SECRET security clearance in connection with his active duty service.

14. From in or about August 1992 through in or about March 2000, **MARTIN** served in the United States Naval Reserve. In or about August 1994, **MARTIN's** security clearance in connection with his Naval service was upgraded to TOP SECRET.

15. Beginning in or about December 1993, and continuing until on or about August 27, 2016, **MARTIN** was employed by at least seven different private companies and was assigned as a contractor to components of DoD and the USIC (collectively, the "government agencies"). **MARTIN** was required to receive and maintain a security clearance in order to work at each of the government agencies to which he was assigned. As a private contractor, **MARTIN** held security clearances up to TOP SECRET/SCI at various times.

16. Over his many years holding a security clearance, **MARTIN** received training regarding classified information, including the definitions of classified information, the levels of classification, and SCI, as well as the proper handling, marking, transportation, and storage of classified materials. **MARTIN** received training on his duty to protect classified materials from unauthorized disclosure, which included complying with handling, transportation, and storage requirements. **MARTIN** knew that unauthorized removal of classified materials and transportation and storage of those materials in unauthorized locations risked disclosure and transmission of those materials, and therefore could endanger the national security of the United States and the safety of its citizens. In particular, **MARTIN** had been advised that unauthorized disclosure of TOP SECRET information reasonably could be expected to cause exceptionally grave damage to the national security of the United States, and that violation of rules governing the handling of classified information could result in criminal prosecution.

17. **MARTIN** worked on a number of highly classified, specialized projects and had access to government computer systems, programs, and information, including classified information.

MARTIN's Theft of National Defense Information

18. Because **MARTIN** held a security clearance and was assigned to various government agencies as a private contractor, the United States Government entrusted **MARTIN** with access to sensitive government materials, including information relating to the national defense that was closely held by the government ("National Defense Information") and classified documents and materials.

19. Beginning at a time unknown, but no earlier than in or about 1996, and continuing through on or about August 27, 2016, **MARTIN** stole and retained U.S. government property, including the documents listed in paragraph 25, below.

20. Many of the documents **MARTIN** stole bore standard markings indicating that they contained highly classified information of the United States, including SECRET and TOP SECRET, as well as SCI, information. The information in the classified documents included National Defense Information.

21. **MARTIN** retained stolen documents, in hard copy and digital form, containing National Defense Information and classified information in a number of locations within his residence and in his vehicle.

22. Martin knew that the stolen documents contained classified information that related to the national defense.

23. **MARTIN** was never authorized to retain these documents at his residence or in his vehicle.

24. **MARTIN** knew that he was not authorized to remove National Defense Information and classified documents from secure locations, was not authorized to retain them at his residence, and was not authorized to retain them in his vehicle.

25. **MARTIN** willfully retained stolen documents that contained National Defense Information, including the following Classified Documents, which were classified as SECRET, TOP SECRET, and SCI:

NSA Documents:

A. A March 2014 NSA leadership briefing outlining the development and future plans for a specific NSA organization.

B. A 2014 NSA report outlining intelligence information regarding foreign cyber issues, containing targeting information.

C. A 2014 NSA report outlining intelligence information regarding foreign cyber issues, containing foreign cyber intrusion techniques.

D. A 2009 draft of a United States Signals Intelligence Directive, which outlined specific methods, capabilities, techniques, processes, and procedures associated with CNO used to defend the United States.

E. February 2008 NSA email correspondence containing an NSA intelligence assessment about an overseas project, containing information directly related to a subject that implicated national security policies and responses.

F. A February 2007 Daily Operations Briefing concerning the daily operations of NSA activities, which identified specific NSA capabilities and operations.

G. A NSA anti-terrorism operational document concerning extremely sensitive U.S. planning and operations regarding global terrorists.

H. 2002 NSA email correspondence and NSA intelligence information regarding extremist activity, which identified targets of intelligence collection.

I. An August 1996 NSA weekly status summary of national defense concerns emanating from various parts of the world.

J. An NSA Threat Operations Center (NTOC) progress report that specifically described activities, capabilities, techniques, process, and procedures associated with NTOC, which discovers, characterizes, and proactively counters threats to U.S. national security systems and other networks of interest.

K. An outline of a classified exercise involving real-world NSA and U.S. military resources to demonstrate existing cyber intelligence and operational capabilities.

L. An NSA User's Guide for an NSA intelligence-gathering tool.

M. A description of the technical architecture of an NSA communications system.

USCYBERCOM Documents:

N. A USCYBERCOM document, dated August 17, 2016, discussing capabilities and gaps in capabilities of the U.S. military and details of specific operations.

O. A USCYBERCOM document, dated August 12, 2016, discussing capabilities and gaps in capabilities of the U.S. military and details of specific operations.

P. A USCYBERCOM document, dated June 9, 2016, containing information about the capabilities and targets of the U.S. military.

Q. A USCYBERCOM document, dated May 23, 2016, containing information about the capabilities and targets of the U.S. military.

R. A USCYBERCOM document, dated August 9, 2007, discussing intelligence sources and method, and the U.S. military's role in a planned counterterrorism operation.

NRO Document:

S. An NRO document, dated August 17, 2007, containing information relating to the launch of an intelligence collection satellite, an unacknowledged ground station, and other specific intelligence collection technologies and programs.

CIA Document:

T. A 2008 CIA document containing information relating to foreign intelligence collection sources and methods, and relating to a foreign intelligence collection target.

The Charges

26. Beginning at times unknown, and continuing until on or about August 27, 2016, each document being a separate Count, in the District of Maryland, and elsewhere, the defendant,

HAROLD T. MARTIN III,

having unauthorized possession of, access to, and control over documents relating to the national defense, willfully retained the documents and failed to deliver them to the officer or employee of the United States entitled to receive them: to wit, **MARTIN** retained documents relating to the national defense at his residence and in his vehicle without authorization, including the documents specified in paragraph 25, above, and listed below:

COUNT	DOCUMENT	AGENCY
ONE	Classified Document A	NSA
TWO	Classified Document B	NSA
THREE	Classified Document C	NSA
FOUR	Classified Document D	NSA
FIVE	Classified Document E	NSA

COUNT	DOCUMENT	AGENCY
SIX	Classified Document F	NSA
SEVEN	Classified Document G	NSA
EIGHT	Classified Document H	NSA
NINE	Classified Document I	NSA
TEN	Classified Document J	NSA
ELEVEN	Classified Document K	NSA
TWELVE	Classified Document L	NSA
THIRTEEN	Classified Document M	NSA
FOURTEEN	Classified Document N	USCYBERCOM
FIFTEEN	Classified Document O	USCYBERCOM
SIXTEEN	Classified Document P	USCYBERCOM
SEVENTEEN	Classified Document Q	USCYBERCOM
EIGHTEEN	Classified Document R	USCYBERCOM
NINETEEN	Classified Document S	NRO
TWENTY	Classified Document T	CIA

18 U.S.C. § 793(e)

FORFEITURE

1. Upon conviction of the offenses in violation of Title 18, United States Code, Section 793(e) set forth in Counts One through Twenty of this Indictment, the defendant, **HAROLD T. MARTIN III**, shall forfeit to the United States of America, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), any property, real or personal, which constitutes or is derived from proceeds traceable to the offenses. The property to be forfeited includes, but is not limited to, the property of the United States seized from the defendant's residence on or about August 27, 2016, and all digital media and devices used to store such information.

2. If any of the property described above, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c).

18 U.S.C. § 981(a)(1)(C)
21 U.S.C. § 853
28 U.S.C. § 2461(c)

Rod J. Rosenstein
United States Attorney

SIGNATURE REDACTED

Foreperson

Date: 2/8/17