UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 14-80031-CR-MARRA(s)(s)

UNITED STATES OF AMERICA

vs.

CHRISTOPHER R. GLENN,

Defendant.
_____/

NOTICE OF FILING EXPERT SUMMARY

The United States hereby gives Notice of its filing of Expert Summary for sentencing. The Expert Summary is attached hereto as Exhibit 1.

Respectfully submitted,

WIFREDO A. FERRER
UNITED STATES ATTORNEY

By: *s/ Ricardo A. Del Toro*
RICARDO A. DEL TORO
Florida Bar No. 0957585
Assistant United States Attorney
99 Northeast 4th Street
Miami, Florida 33132-2111
Tel: (305) 961-9182
Fax: (305) 536-4675
Ricardo.Del.Toro@usdoj.gov

CHRISTIAN E. FORD
Trial Attorney
Counterintelligence and Export Control Section
National Security Division
United States Department of Justice
Tel: (202) 233-2049

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a true and correct copy of the foregoing was filed by CM/ECF on July 27, 2015.

s/ Ricardo A. Del Toro
RICARDO A. DEL TORO
Assistant United States Attorney

Exhibit 1

EXPERT SUMMARY
GERALD PARSONS

Area of Expertise: Computer forensic digital analysis

Basis for Testimony:

- Thirteen (13) years of forensic analysis experience working as chief of two military counterintelligence cyber teams.

- Professional certifications as a certified computer forensic examiner, certified information systems security professional, computer crime investigator, digital forensic certified practitioner, certified ethical hacker, and EnCase certified examiner, among others.

- Extensive and numerous digital forensics courses including network exploitation techniques, live network investigations, network monitoring, forensic investigations in Windows, Linux, Solaris and MacIntosh Apple OSX examinations, among others.

Reliability of Principles and Methods: Mr. Parsons uses principles and methods which are generally accepted in the field of computer forensic and digital analysis. Those methods include imaging of the computers and removable storage media such as DVDs, hard drives and CDs containing digital files and ensuring their integrity by obtaining and comparing MD-5 Hash values that provide a digital "fingerprint" used to verify the authenticity of the image. Additional methods used are the examination of logical and physical files stored on computers and storage media; and the examination of system files that reveal programs that were run on a system as well as files that were changed on the system. The goal of most of these examinations is to find files with probative information and to discover information about when and how these files came to be on the computer or storage media.

Purpose of Presenting Mr. Parson's Testimony: To provide an explanation of the defendant's actions with respect to computers, removable media and digital evidence obtained during the course of the investigation of this case, including the steps that the defendant took to obtain without authorization, copy onto removable media and an encrypted volume within a computer storage device (Synology Network Attached Storage) and the steps that the defendant took to try to conceal his actions. Additionally, Mr. Parsons will also explain how the system files contained within a government classified (SIPR) hard drive and a government unclassified (NIPR) hard drive revealed additional evidence of defendant's computer intrusion, unauthorized taking of classified and unclassified information and the steps he took to conceal those actions.

Summary of Proposed Testimony: Mr. Parsons will describe his imaging and forensic analysis of SIPR and NIPR hard drives, multiple DVDs, a Synology NAS computer storage device and numerous system files located within the JTF-B computers at Soto Can Air Base, Honduras. Mr.

Parsons will describe his analysis of logical and physical files located within the examined devices as well as information obtained from system files that yielded probative evidence of when and how certain files came to be on the computers and storage media examined. Mr. Parsons will also compare and contrast his forensic findings with a number of explanations that defendant has given about what he did, how he did it and his motive for taking those actions with respect to the charged computer intrusion and espionage offenses.

Conclusion: Mr. Parsons will opine that the defendant intentionally and methodically set out to take without authorization numerous classified and unclassified documents and files, copied them onto removable media and then re-copied them in an encrypted format onto a hidden digital compartment within a Synology computer storage device in his Honduras residence; that the defendant took various steps to try to conceal his actions including mass deletion of system files, and deletion of security event logs after copying stolen classified files onto a DVD; that the defendant used password cracking and wiretapping utilities and set up a digital tunnel that allowed him to breach the JTF-B firewall security protocols to send and receive information from outside the JTF-B without authorization in an effort to circumvent security controls; that the likely effect of shutting down the Synology storage device before law enforcement could access it would be to make it more difficult for law enforcement forensic experts to remotely access the device; that forensic analysis of the Synology device revealed that the stolen classified files were likely copied again from the Synology device in November 2012; and that the totality of the circumstances suggest that the defendant engaged in a systematic pattern of security violations, theft of classified and sensitive military materials and concealment.