**Summary of Search Conducted by the Treasury Inspector General for Tax Administration (TIGTA)**

***Privacy International v. Federal Bureau of Investigation*, 18-376 (D.D.C.)**

* Plaintiff’s Freedom of Information Act request was dated and received by the Treasury Inspector General for Tax Administration (TIGTA) on September 10, 2018.
* Plaintiff’s FOIA request sought records pertaining to law enforcement hacking.
* Upon reviews of Plaintiff’s FOIA request, TIGTA’s FOIA Branch determined, based upon its general knowledge of the functions and records maintained in each of the functions, that TIGTA’s Office of Investigations, Office of Deputy Inspector General for Audit, Office of Deputy Inspector General for Inspections and Evaluations, and Office of Information Technology were most likely to have custody of records potentially responsive to the Plaintiff’s FOIA request.
* On Wednesday, September 12, 2018, a request was made to the Office of Investigations, Office of Deputy Inspector General for Audit, Office of Deputy Inspector General for Inspections and Evaluations, and Office of Information Technology to search for responsive records.
* Office of Investigations (OI): Based upon the experience of the staff of the Office of Investigations, TIGTA conducted a structured query language (SQL) query of the Criminal Results Management System (CRIMES), the database that tracks and indexes the casework performed by all of OI’s investigative units, including the casework of the Forensic and Digital Science Laboratory, the Strategic Data Services Division, the Criminal Intelligence and Counterterrorism Division, and the Cybercrimes Investigations Division. The search was limited to complaints or investigations relating to identified TIGTA or Internal Revenue Service Criminal Investigation subjects in which computer hacking techniques were mentioned in either of CRIMES’ narrative fields. There were no date parameters used when performing this query, thus all available data within CRIMES was searched.
  + The following search terms were used to conduct the query:
* Basis has 'Network Investigation Technique'
* OR Basis has 'NIT '
* OR Basis has 'Computer Network Exploitation'
* OR Basis has 'CNE '
* OR Basis has 'Computer and Internet Protocol Address Verifier'
* OR Basis has 'CIPAV '
* OR Basis has 'Internet Protocol Address Verifier'
* OR Basis has 'IPAV '
* OR Basis has 'Remote Access Search and Surveillance'
* OR Basis has 'RASS '
* OR Basis has 'Remote Computer Search'
* OR Basis has 'Remote Access Search'
* OR Basis has 'Remote Search'
* OR Basis has 'Web Bug'
* OR Basis has 'Sniffer'
* OR Basis has 'Computer Tracer'
* OR Basis has 'Internet Tracer'
* OR Basis has 'Remote Computer Trace'
* OR Basis has 'Hacking'
* OR Basis has 'Extraordinary Access'
* OR Basis has 'Equipment Interference'
* OR Basis has 'Trojan'
* OR Basis has 'Magic Lantern'
* OR Basis has 'Malware'
* OR Basis has 'Spyware'
* OR Basis has 'Worms'
* OR Basis has 'Virus'
* Results has 'Network Investigation Technique'
* OR Results has 'NIT '
* OR Results has 'Computer Network Exploitation'
* OR Results has 'CNE '
* OR Results has 'Computer and Internet Protocol Address Verifier'
* OR Results has 'CIPAV '
* OR Results has 'Internet Protocol Address Verifier'
* OR Results has 'IPAV '
* OR Results has 'Remote Access Search and Surveillance'
* OR Results has 'RASS '
* OR Results has 'Remote Computer Search'
* OR Results has 'Remote Access Search'
* OR Results has 'Remote Search'
* OR Results has 'Web Bug'
* OR Results has 'Sniffer'
* OR Results has 'Computer Tracer'
* OR Results has 'Internet Tracer'
* OR Results has 'Remote Computer Trace'
* OR Results has 'Hacking'
* OR Results has 'Extraordinary Access'
* OR Results has 'Equipment Interference'
* OR Results has 'Trojan'
* OR Results has 'Magic Lantern'
* OR Results has 'Malware'
* OR Results has 'Spyware'
* OR Results has 'Worms'
* OR Results has 'Virus’

The search was conducted with negative results and OI provided the results in response to the search request.

TIGTA OI further reported that it is unaware of any instance in which it investigated another Government agency for the use of technical duplicity, malicious software, or other electronic subterfuge to break into a subject of an investigation’s protected media without the subject’s knowledge.

* Office of Inspections and Evaluations (I&E) . Based upon the experience of the staff of the Office of Inspections and Evaluations, TIGTA conducted an electronic search of TeamMate suite of applications, I&E’s sharepoint site, and the Staff Advisor’s shared drawer, using the terms “hacking” and “phishing” and visually scanning the results. The search was conducted with negative results. I&E provided a response to the search request that it had no responsive records.
* Office of Audit (OA). Based upon the knowledge of the Deputy Inspector General for Audit (DIGA) and the Assistant Inspector General for Audit, Security and Information Technology Services (AIGA/SITS) regarding current and past audit worked conducted by OA, OA provided a response to the search request that it did not have any responsive documents.
* Office of Information Technology (OIT). Based upon the experience of the staff of the Office of Information Technology that OIT does not support any execution of hacking techniques, OIT provided a negative response to the search request.