FD-1057 (Rev. 5-8-10)

[redacted]

OFFICIAL RECORD
Document participants have digitally signed. All signatures have been verified by a certified FBI information system.

FEDERAL BUREAU OF INVESTIGATION

Electronic Communication

Title: [redacted] Opening EC - ALFA BANK **Date:** 09/23/2016

CC: JONATHAN C. MOFFA
Joe Pientka III
John F. Stofer
Paul M. Maric
STRZOK PETER P II

From: CHICAGO
CG-CY-1
Contact: Allison Sands, 312-829-8628

Approved By: SSA Daniel S. Wierzbicki
A/CDC STEVEN MOLESKY
ASAC John A. Brown
SAC Michael J. Anderson

Drafted By: Allison Sands
Curtis A. Heide

Case ID #: [redacted] [redacted] ALFA BANK;
FCI RUSSIA - CONTACTS / AGENTS
SENSITIVE INVESTIGATIVE MATTER

Synopsis: [redacted] Documents the opening of a Full Field Investigation into the network communications between a US-based server and the Russian ALFA BANK organization.

Reason: 1.4(b)
Derived From: National Security Information SCG
Declassify On: 20261231

Full Investigation Initiated: 09/23/2016

Enclosure(s): Enclosed are the following items:
1. (U//FOUO) White Paper

[redacted]

[redacted]

Title: [redacted] Opening EC - ALFA BANK
Re: [redacted], 09/23/2016

Details:

[redacted] On or about September 19, 2016, FBI received a referral of information from the US DEPARTMENT OF JUSTICE, detailing an unusually configured email server in Pennsylvania belonging to the TRUMP ORGANIZATION. In that referral, the DEPARTMENT OF JUSTICE provided the FBI with a whitepaper that was produced by an anonymous third party. According to the whitepaper, a U.S.-based server that is owned by the TRUMP ORGANIZATION has been communicating with the Russian-based ALFA BANK organization in Moscow, Russia. The third party identified that some of the communications were utilizing a TOR node, which is a means of obfuscating a user's true network location on the Internet. The TOR node was identified at an organization called SPECTRUM HEALTH, located in the State of Michigan. Additionally, the servers are reportedly configured for direct and exclusive communication between the TRUMP ORGANIZATION and the ALFA BANK entity. Additional details from the predicating report are listed as follows:

[redacted] On approximately July 28, 2016, a lookup in global DNS returned 15 unique hostnames containing "mail," "smtp," "relay," or "mta" that were registered to the TRUMP ORGANIZATION. A computerized and manual scan revealed anomalous data on one the the domains: mail1.trump-email.com [IP address 66.216.133.29]. An open source WHOIS lookup confirmed that the parent domain for mail1.trump-email.com is registered to the TRUMP ORGANIZATION.

[redacted] In the 90 day period May 4, 2016 to September 4 2016, only 19 external IP addresses conducted an A Record search for mail1.trump-email.com, a much smaller number of IP addresses than expected in normal traffic. Of the 19 IP addresses, the vast majority of the lookups came from the same three IP addresses: 217.12.97.15 [ALFA BANK], 217.12.96.15 [ALFA BANK], 167.73.110.8 [SPECTRUM HEALTH]. The SPECTRUM HEALTH IP address has been identified as a TOR exit node that is used exclusively by the Russian ALFA BANK entity. Notably, the majority of the lookups for this mail server by ALFA BANK were not for the MX [mail record], indicating that the server was set up to

masquerade as a regular (non-mail) server. Also, mail1.trump-email.com is configured to only accept email from pre-approved IP addresses.

[redacted] Based on the information above, FBI Chicago has predicated a Full Field Counterintelligence investigation into the activities of ALFA BANK, in order to conduct further investigation regarding the extent and nature of the network communications between ALFA BANK and the TRUMP ORGANIZATION. This investigation will attempt to determine the validity of the information that was provided by the third-party entity, and to assess whether or not pose a threat to either the TRUMP ORGANIZATION, or United States national security.

[redacted] In addition, FBI investigation [redacted] [CROSSFIRE HURRICANE] was predicated based on an allegation that a member of the TRUMP campaign had received a suggestion from the Russian Government, indicating that the Russian government could assist the TRUMP campaign with an anonymous release of information during the campaign, which would be a detriment to the HILLARY CLINTON campaign. Investigation in [redacted] has surfaced additional ties between the TRUMP campaign team and the Russian government.

[redacted] Investigation of the communications between the Russian ALFA BANK and the TRUMP ORGANIZATION could provide additional insight about the connections between the TRUMP ORGANIZATION and Russia, and help to determine whether those ties pose a threat to United States national security.

[redacted] This matter is being treated as a Sensitive Investigative Matter based on the fact that the TRUMP ORGANIZATION is affiliated with a current U.S. Presidential candidate. As such, FBI Chicago requests that FBIHQ/NSLB coordinate with the US DEPARTMENT OF JUSTICE to provide all appropriate notifications required by the DIOG.

♦♦