U.S. Department of Justice

National Security Division

Washington, D.C. 20530

December 6, 2017

F. Whitten Peters, Esquire
Steven M. Cady, Esquire
Williams & Connolly LLP
725 12th Street, N.W.
Washington, D.C. 20005

Re: Netcracker Technology Corporation Non-Prosecution and Security Agreement

Dear Counsel:

The United States Department of Justice ("DOJ"), National Security Division, and the United States Attorney's Office for the Eastern District of Virginia (collectively, the "Offices"), have investigated Netcracker Technology Corporation (the "Company" or "NTC"), a corporation organized under the laws of Massachusetts and headquartered in Massachusetts, regarding matters described in the Statement of Facts, attached hereto as Attachment A. The Offices and NTC (the "Parties") have reached a mutual agreement to resolve the investigation and enhance the security of U.S. telecommunications networks by limiting information that will be sent to, stored in, or accessed from overseas locations. Among the factors considered in entering into this agreement were:

a) NTC is a software engineering firm that offers network solutions that enable large corporations to optimize network communications and operations. NTC's global clientele includes telecommunications companies and large enterprises.

b) Like many software companies, NTC and its subsidiaries develop software using foreign technical personnel in the United States and in a number of foreign countries.

c) The use of a global technical workforce for the creation of software and the provision of related services, while a common and valuable business practice, create concerns for the security of sensitive individual data, sensitive network data, and critical U.S. domestic communications infrastructure. For example, electronic communications to and from Russia are subject to the Russian System of Operative-Investigative Measures ("SORM"). SORM authorizes the Federal Security Service of the Russian Federation ("FSB") to collect, analyze, and store information transmitted on Russian telecommunications networks.

d) Given the cyber threat posed by foreign government security agencies and cyber criminals, many based offshore, the Offices entered into discussions with NTC about

steps that could be taken to minimize risks to sensitive individual data, sensitive network data, and critical U.S. domestic communications infrastructure while retaining the value of using a global workforce.

e) In response to the threat, NTC agreed to implement an Enhanced Security Plan, attached hereto as Attachment B, which the Offices believe will substantially improve the security of NTC's software and any software that is developed using foreign technical workers operating overseas and in the United States. The new security structure will limit the information that will be sent to, stored in, or accessed from overseas locations, and provides protocols for removing or obscuring sensitive data.

f) The Enhanced Security Plan advances industry best practices for protecting sensitive information about U.S. telecommunications networks, and is a model that other companies should follow in connection with critical infrastructure applications.

In light of NTC's assistance in protecting sensitive individual data, sensitive network data, and critical U.S. domestic communications infrastructure by implementing the Enhanced Security Plan at NTC's expense, the Offices have decided to close the investigation and assess no penalty, provided that NTC complies with this Non-Prosecution Agreement ("Agreement") and the Enhanced Security Plan.

NTC and the Offices agree to work together on a press release reflecting these principles, and NTC agrees that if it or any of its direct or indirect subsidiaries or affiliates issues a press release or holds any press conference in connection with this Agreement, the Company shall first consult the Offices to determine (a) whether the text of the release or proposed statements at the press conference are true and accurate with respect to matters between the Offices and the Company, and (b) whether the Offices have any objection to the proposed release or statement. In the event of an objection by the Offices to any proposed release or statement by NTC, NTC agrees not to issue the release or statement unless the Offices' objection has been resolved to the Offices' satisfaction.

This Agreement is made by the Company and the Offices as of the date of the last signature affixed hereto ("Effective Date").

1. Non-Prosecution

In an effort to resolve the investigation referenced above and to protect U.S. national security from unauthorized access to U.S. telecommunications networks, (a) NTC voluntarily agrees that it will abide by the provisions set forth in this Agreement and in the Enhanced Security Plan, attached hereto as Attachment B, for the time periods set out below, and (b) the Offices agree that they will not prosecute NTC, or any of its present or former officers or employees, for any criminal wrongdoing (except as provided herein and except for any tax matters, as to which the Offices cannot as a matter of policy make any agreement) relating to any allegation investigated by the Offices, including the conduct described in Attachment A.

The Offices, however, may use any information related to the matters described in this Agreement, including Attachment A, against the Company: (a) in a prosecution for perjury or obstruction of justice in connection with the investigations described above; (b) in a prosecution for making a false statement in connection with the investigations described above; (c) in a prosecution or other proceeding relating to any crime of violence; or (d) in a prosecution or other proceeding relating to a violation of any provision of Title 26 of the United States Code (the

Internal Revenue Code). This Agreement does not provide any protection against prosecution for any future conduct by the Company or its officers.

In the event the Offices determine that the Company has breached this Agreement, the Offices agree to provide the Company with written notice of such breach prior to taking any action pursuant to Section 2.A or Section 4.B of this Agreement resulting from such breach. Within thirty (30) days of receipt of such notice, the Company shall have the opportunity to respond to the Offices in writing to explain the nature and circumstances of such purported breach, as well as the actions the Company has taken to address and remediate the situation, which explanation the Offices shall consider in determining whether to pursue prosecution of the Company under Section 2.A of this Agreement and/or pursue liquidated damages under Section 4.B of this Agreement.

In the event that the Offices determine that the Company has breached this Agreement: (a) all statements made by or on behalf of the Company to the Offices, including Attachment A, and any testimony given by the Company before a grand jury, a court, or any tribunal, or at any legislative hearings, whether prior or subsequent to this Agreement, and any leads derived from such statements or testimony, shall be admissible in evidence in any and all criminal proceedings brought by the Offices against the Company; (b) the Company shall not assert any claim under the United States Constitution, Rule 11(f) of the Federal Rules of Criminal Procedure, Rule 410 of the Federal Rules of Evidence, or any other federal rule that any such statements or testimony made by or on behalf of the Company prior to this Agreement, or any leads derived therefrom, should be suppressed or are otherwise inadmissible; and (c) the Company shall pay liquidated damages in accordance with the processes outlined in Section 4.B of this Agreement.

Any prosecution against the Company may be premised on any non-privileged information provided by the Company. The decision whether conduct or statements of any current director, officer, or employee, or any person acting on behalf of, or at the direction of, the Company, will be imputed to the Company for the purpose of determining whether the Company has violated any provision of this Agreement shall be in the sole discretion of the Offices.

2. Three-Year Term Provisions

NTC voluntarily agrees that it will abide by the provisions set forth in this Section 2 of this Agreement for a term of three years from the Effective Date ("Three-Year Term").

A. **Future Prosecution.** If, during the Three-Year Term, the Company (a) provides in connection with this Agreement deliberately false, incomplete, or misleading information; or (b) fails to implement the Enhanced Security Plan as set forth in this Agreement and Attachment B, the Company and its officers and employees shall thereafter be subject to prosecution for any federal criminal violation of which the Offices have knowledge obtained through non-privileged sources, including, but not limited to, the conduct described in this letter and Attachment A, which may be pursued by the Offices in the U.S. District Court for the Eastern District of Virginia or any other appropriate venue. Subject to the provisions set out in Section 7 of Attachment B, determination of whether the Company or any of its officers or employees has breached this Agreement and whether

to pursue prosecution of the Company or any of its officers or employees shall be in the Offices' sole discretion.

B. Reporting Illegal Conduct.

(i) Reporting Violations. During the Three-Year Term, should the Company learn of credible evidence of a felony violation of U.S. law involving fraud or compliance with U.S. export control laws, the Company shall promptly report such evidence or allegations to the Offices, and the Company shall truthfully disclose all factual information not protected by a valid claim of attorney-client privilege or work product doctrine with respect to such evidence or allegations. This obligation of truthful disclosure includes, but is not limited to, the obligation of the Company to provide to the Offices, upon request, any non-privileged document, record, or other tangible evidence related to such evidence or allegations about which the Offices may inquire of the Company.

(ii) Provision of Information and Testimony. Upon request of the Offices, the Company shall designate knowledgeable employees, agents, or attorneys to provide to the Offices non-privileged information and materials relating to any report of violation under this Section 2.B. It is further understood that the Company must at all times provide complete, truthful, and accurate information. The Company shall use its best efforts to make available for interviews or testimony, as requested by the Offices, present or former officers, directors, employees, agents, and consultants of the Company who have knowledge of the reported violation. This obligation includes, but is not limited to, sworn testimony before a federal grand jury or in federal trials, as well as interviews with domestic or foreign law enforcement and regulatory authorities. Cooperation shall include identification of witnesses who, to the knowledge of the Company, may have material information regarding the matters under investigation. With respect to any information, testimony, documents, records, or other tangible evidence provided to the Offices during the Three-Year Term pursuant to this Agreement, the Company consents to any and all disclosures, subject to applicable law and regulations, to other governmental authorities, including United States authorities and those of a foreign government, of such materials as the Offices, in their sole discretion, shall deem appropriate.

(iii) Certification. No later than 90 days prior to the expiration of the Three-Year Term, the Company, by the Chief Executive Officer of the Company, the Chief Financial Officer of the Company, and the Security Director, will certify to the Offices that the Company has met its disclosure obligations pursuant to this Agreement. Such certification will be deemed a material statement and representation by the Company to the Executive Branch of the United States for purposes of 18 U.S.C. § 1001.

C. Contracting. During the Three-Year Term, NTC agrees to seek the non-objection of the Offices prior to bidding for any new federal, state, or local government prime contract or subcontract. NTC may complete the bidding process while awaiting a decision from the Offices. This requirement also applies to bids NTC submits to current government clients for new work. The Offices shall not object to any new NTC bid without cause, and shall provide an explanation of the reason(s) for an objection, unless and to the extent an objection is based on classified or law enforcement-sensitive information that cannot be shared. Within thirty (30) days of the Effective Date, NTC shall submit to the Offices a list

of any such government contracts that pre-date the Effective Date. That list shall specify the name of the client as well as the nature of the work performed.

3. Seven-Year Term Provisions

NTC voluntarily agrees that it will abide by the provisions set forth in this Section 3 of this Agreement for a term of seven years from the Effective Date ("Seven-Year Term").

A. Enhanced Security Plan for U.S.-Based Domestic Communications Infrastructure. The Company shall implement and maintain an enhanced security and risk assessment and remediation program based upon recognized national and/or international security standards or guidelines and best practices for U.S.-Based Customers' Domestic Communications Infrastructure as set forth in Attachment B ("Enhanced Security Plan").

B. Third-Party Auditor. The Company agrees to retain an independent, third-party auditor ("Third-Party Auditor") to review and assess in a professionally independent and objective fashion NTC's processes, policies, and procedures related to, and NTC's compliance with, its Enhanced Security Plan as set forth in Attachment B. The qualifications of the Third-Party Auditor and procedures for selecting the Third-Party Auditor are set out in Section 6 of Attachment B.

C. Reports. The reports required by this Section 3 will likely include proprietary, financial, confidential, and competitive business information. Moreover, public disclosure of the reports could discourage cooperation and impede pending or potential government investigations and, thus, undermine the objectives of the reporting requirement. For these reasons, among others, the reports and the contents thereof are intended to remain and shall remain non-public, except as otherwise agreed to by the parties in writing, or except to the extent required by law.

(i) Annual Reports. The Company agrees to make annual reports to the Offices on the status of its implementation, operation, and effectiveness of the controls and procedures set out in Attachment B, one year after the Effective Date and at one-year intervals thereafter, in accordance with the Enhanced Security Plan. The Company may extend the time period for submission of any of the annual reports with prior written approval of the Offices. The Company shall endeavor to respond promptly to any inquiries from the Offices relating to the content of an annual report.

(ii) Final Report. The Company agrees to provide a final review and report to the Offices summarizing the progression of the implementation, operation, and effectiveness of the controls and procedures set out in Attachment B ("Final Report"). The Final Report shall be completed and delivered to the Offices no later than forty-five (45) days before the expiration of the Seven-Year Term.

D. Reporting Violations. Should the Company discover credible evidence of (1) an actual or attempted circumvention of the security protocols in Attachment B, (2) failure to follow the security protocols in Attachment B, or (3) any unauthorized access to any system

maintained by NTC that would impair or impede the security protocols in Attachment B, then NTC shall report such events to the Offices within five (5) days.

E. Foreign Legal Process. The Company shall not breach the Enhanced Security Plan in responding to the legal process of, or a request from or on behalf of a foreign government, identified representative, component or subdivision thereof, without the express written consent of the Offices or the authorization of a court of competent jurisdiction in the United States. Any such legal process or request that would result in actual or attempted circumvention of the Enhanced Security Plan shall be reported to the Offices as soon as possible and in no event more than five (5) days after NTC becomes aware of the process or request. NTC shall take reasonable measures to ensure that it will learn of all such requests or submission of legal process. Further, NTC shall notify the Offices in writing within 30 days of receipt of legal process or requests from foreign non-governmental entities for actions that would constitute a breach of the Enhanced Security Plan, unless the disclosure of the legal process or requests would be in violation of an order of a court of competent jurisdiction within the United States.

F. Other Compliance Programs. The Company shall implement and maintain an effective compliance and ethics program that fully comports with the criteria set forth in Section 8B2.1 of the United States Sentencing Guidelines Manual (the "Compliance & Ethics Program"). As part of the Compliance & Ethics Program, NTC shall maintain a permanent compliance office and a permanent education and training program relating to the laws, regulations, and ethics governing the work of the Company, paying particular attention to NTC's procurement and subcontracting practices. As part of the Compliance & Ethics Program, NTC shall (a) ensure that an effective program be maintained to detect and punish violators of laws, policies, and standards, and encourage those who report such violators; (b) ensure that no employee or agent of NTC is penalized in any way for providing information relating to NTC's compliance or noncompliance with laws, policies, and standards to any NTC official, government agency, compliance officer, and/or the Third-Party Auditor; and (c) ensure that all NTC employees have access to a hotline or other means to provide information to NTC's compliance office relating to NTC's compliance or noncompliance with laws, policies, and standards. On at least an annual basis, NTC shall take steps to assess the Compliance & Ethics Program to ensure it is carrying out the duties and responsibilities set out in this Agreement.

4. Security Enhancement Investment and Liquidated Damages

A. Necessary Funds. NTC will invest the funds necessary to enhance cyber and data security for itself and the work it does for its clients in accordance with the Enhanced Security Plan, attached hereto as Attachment B.

B. Liquidated Damages.

(i) Process for Finding Breach. The Offices shall determine, in their sole discretion, whether NTC has materially breached this Agreement, including failure to comply with any part of the Enhanced Security Plan. A material breach may constitute a single event or a series of events grouped collectively.

(ii) Process for Imposing Liquidated Damages after a Breach. The Parties agree that if the Arbiter, as described below, determines that NTC materially breached this Agreement (including by failing to comply with the Enhanced Security Plan), then NTC shall pay an amount of $35 million in liquidated damages to the United States Treasury according to the following procedures:

a. As provided above in Section 1 of this Agreement, upon written notification to NTC by the Offices of a material breach, the Company shall have thirty (30) days to respond in writing as to the nature of the breach and any remediation. During this time, the Parties shall attempt in good faith to negotiate a resolution of the material breach.

b. If the Parties are unable to reach a resolution within thirty (30) days, the Parties shall negotiate in good faith to identify a neutral third-party arbiter (the "Arbiter") to resolve the dispute. The Arbiter shall hold a security clearance or be capable of obtaining a security clearance. Each Party shall provide a list of at least three Arbiter candidates. The Parties shall agree on an Arbiter within ten days. In the event the Parties are unable to reach agreement on an Arbiter, the Offices and NTC shall each nominate one individual from the two lists of Arbiter candidates, and those two people shall within five (5) days select the Arbiter from the previously exchanged lists of candidates.

c. The sole issues for determination by the Arbiter, which the Offices must prove by a preponderance of evidence, are (i) whether the Offices' determination of a breach was supported by the evidence, and (ii) whether the breach was a material breach of the Agreement. For purposes of this proceeding, NTC stipulates that liquidated damages of $35 million are reasonable in the event of a material breach of the Agreement. Within ten days of selecting an Arbiter, a preliminary conference will be held and the agenda for that conference and timelines for the remainder of the proceeding will be set by the Arbiter. Within 20 days of the preliminary conference, the Arbiter will hold an evidentiary hearing on the merits and the Parties will present argument. This hearing shall last no more than eight hours, with each side allotted equal time for presentation of direct evidence, which may be submitted by way of documents, direct examinations, written declarations, and cross-examination. Briefing, not to exceed 10 pages per Party, may be submitted by either Party on or before the day of this hearing, as determined by the Arbiter. The Arbiter shall issue a brief, reasoned decision as to (i) whether the determination of breach by the Offices was supported by the evidence, and (ii) whether the breach was material. The decision shall be rendered in writing within 15 days of the close of the hearing. The Parties agree that the decision of the Arbiter shall be final, with no right to appeal, and shall not be subject to judicial review, including claims under the Administrative Procedure Act or any provision of the Constitution. The Parties shall maintain the confidential nature of the proceeding. All fees owed to the Arbiter will be paid by NTC.

d. The Offices shall file with the Arbiter an administrative record, which shall consist of the information (both classified and unclassified) that the Offices intend to rely upon to support the Office's action under review. All unclassified information contained in the administrative record that is not otherwise privileged or subject to

statutory protections shall be provided to NTC. No discovery shall be permitted. NTC may also submit information to the Arbiter as part of the administrative record, and that information shall be provided to the Offices. The Offices may provide classified information to the Arbiter and to NTC (for example to sufficiently cleared counsel) as part of the administrative record. Alternatively, the Offices may submit classified information that cannot be shared with NTC to the Arbiter *ex parte* and *in camera* for inclusion in the administrative record. For this category of classified information, the Offices shall provide an unclassified summary of the classified information to NTC's counsel pursuant to a protective order, taking into account the circumstances of the case, including NTC's ability to respond to the action at issue, unless the head of the department or agency whose classified information is at issue, or his or her designee, determines in his or her discretion that providing a summary could damage the national security of the United States. In this event, the Arbiter may consider the inability of NTC to review and respond to classified information in the administrative record in making a final determination.

e. If the Arbiter decides, in writing, that the determination of breach by the Offices was supported by the evidence, and that the breach was material, then NTC shall pay the amount of $35 million to the United States Treasury within ten days of such written determination.

f. The rights of the Parties for the purpose of the liquidated damages determination not already addressed under this Agreement shall be governed by and construed in accordance with the laws of the District of Columbia, exclusive of conflict or choice of law rules.

(iii) Consecutive Breach Findings. A single determination of breach by NTC shall not preclude subsequent determinations by the Offices of another breach by NTC, but the assessment of the liquidated damages award by the Arbiter in the event of a material breach by NTC shall occur only once.

5. General Provisions

A. Work for U.S. Telecommunications Companies. By adhering to this Non-Prosecution Agreement and implementing the Enhanced Security Plan, which is based on recognized security standards and current best practices, the Offices agree that Netcracker can achieve the necessary security organization and operational controls the Offices expect of a company with sensitive access to critical U.S. domestic communications infrastructure.

B. Enforceability. This Agreement is binding on the Company and the Offices but specifically does not bind any other federal agencies, or any state, local, or foreign law enforcement or regulatory agencies, or any other authorities, although the Offices will bring the cooperation of the Company and its compliance with its other obligations under this Agreement to the attention of such agencies and authorities if requested to do so by the Company.

C. Company Successors. This Agreement shall be binding upon any successor (whether direct or indirect and whether by purchase, lease, merger, consolidation,

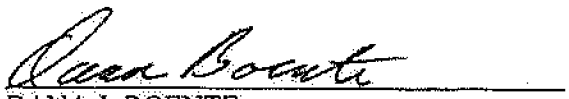
liquidation or otherwise) to all or substantially all of the Company's business and/or assets. The provisions of this paragraph shall apply to NTC's parent company to the extent that NTC's parent company absorbs any NTC assets or corporate departments, assumes NTC functions, or otherwise acts as a successor of NTC, notwithstanding the exemption described in Section 1.h of the Enhanced Security Plan. Any such successor will within a reasonable period of becoming the successor assume in writing and be bound by all of the Company's obligations under this Agreement. For all purposes under this Agreement, the term "Company" shall include any successor to the Company's business or assets that becomes bound by this Agreement.

D. Disclosure. It is further understood that the Company and the Offices may disclose this Agreement to the public, including Attachments A and B.

E. Communications. All reports and notices required under this Agreement shall be sent to: Deputy Chief – Cyber, Counterintelligence and Export Control Section, National Security Division, U.S. Department of Justice, 950 Pennsylvania Avenue, N.W., Washington, D.C. 20530; Chief, Foreign Investment Review Staff, National Security Division, U.S. Department of Justice, 600 E Street, N.W., 10th Floor, Washington, D.C. 20004; and to Chief – Cybercrimes Unit, United States Attorney's Office for the Eastern District of Virginia, 2100 Jamieson Avenue, Alexandria, VA 22314.

F. Modification. This Agreement sets forth all the terms of the Agreement between the Company and the Offices. No amendments, modifications, or additions to this Agreement shall be valid unless they are in writing and signed by the Offices, the attorneys for the Company, and a duly authorized representative of the Company.

Sincerely,



DANA J. BOENTE
Acting Assistant Attorney General

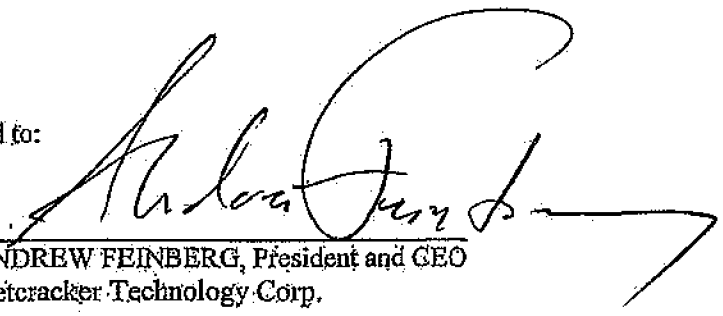
David H. Laufman, Chief
Counterintelligence and Export Control Section

Heather M. Schmidt, Senior Trial Attorney
Counterintelligence and Export Control Section

Richard C. Sofield, Principal Deputy Chief
Foreign Investment Review Staff

DANA J. BOENTE
United States Attorney
Eastern District of Virginia

Agreed to:

By: 

ANDREW FEINBERG, President and CEO
Netcracker Technology Corp.

ATTACHMENT A

STATEMENT OF FACTS

The following Statement of Facts is incorporated by reference as part of the Non-Prosecution and Security Agreement (the "Agreement") between the United States Department of Justice, National Security Division, the United States Attorney's Office for the Eastern District of Virginia (collectively, the "Offices"), and Netcracker Technology Corporation ("NTC"). The Offices investigated allegations relating to a Defense Information Systems Agency ("DISA") contract, NTC's compliance with the International Traffic in Arms Regulations ("ITAR") administered by the State Department and with Export Administration Regulations ("EAR") administered by the Department of Commerce, and NTC's compliance with immigration laws. Although NTC denies that it engaged in any criminal wrongdoing, in the interest of reaching a mutual agreement to resolve the investigation and enhance U.S. national security, NTC and the Offices agreed, among other things, to the following Statement of Facts and to enter into an Enhanced Security Plan, which is Attachment B to the Agreement.

CORPORATE BACKGROUND

NTC is a software engineering firm offering network solutions to enable large corporations to optimize network communications and operations. NTC's flagship software product streamlines business support systems and operations support systems in a single platform approach to enable large corporations to optimize network communications and operations. NTC's global clientele includes telecommunications providers and large enterprises.

NTC sells licenses to its Commercial Off the Shelf ("COTS" or "core") products, and enters into services contracts to provide customization, configuration, and implementation services, which NTC refers to internally as customer specific "projects." NTC and its subsidiaries employ technical personnel in the United States and in a number of foreign countries, including Belarus, Brazil, India, Latvia, Russia, Ukraine, and the United Kingdom. Personnel from NTC's foreign offices frequently travel to the United States in connection with customer projects in the United States.

THE DISA CONTRACT

DISA oversees and manages the Defense Information System Network ("DISN"), which provides a consolidated worldwide telecommunications infrastructure to the United States Department of Defense ("DoD"). The DISN runs data, voice, optical, satellite, and phone services on both classified and unclassified networks, including SIPRNet, the U.S. Government's Secret-level network. Given the defense-related, classified, and sensitive information flowing over these networks, DISA's network architecture relies on a variety of classified, controlled, and sensitive technologies. Some technical requirements and specifications of the DISN are sensitive and/or classified.

In late 2007, NTC entered into negotiations to provide both software and services to DISA. NTC offered its core commercial software product to DISA for use on both DISA's Secret-level network and DISA's unclassified network. To enable NTC's product to interface with the networks run by DISA, the core product had to be customized. DISA ultimately entered into a licensing contract for NTC's core commercial product. From the beginning of its negotiations with NTC, DISA was aware the core product had been developed by NTC using programmers in Russia and Ukraine. For that reason, the U.S. government evaluated whether this core product would introduce

vulnerabilities into government networks. In June 2008, based on representations made by NTC and the U.S. government's evaluation, DISA determined that use of the core product on government networks was acceptable and approved the core product for purchase and customization as described below. The licensing agreement between DISA and NTC provided that all customization work that NTC did for DISA would be the property of NTC and could be used in future versions of NTC's core product.

The second contract between DISA and NTC was a multi-year services project (the "DISA Project") to customize and configure the core code, including subsequent changes to the core code, for implementation in the DISN's unique systems. During the negotiation period from late 2007 through September 2008, DISA sought and received certifications from NTC that, among other things, "all [NTC] employees assigned to the project will be U.S. citizens" and that "only [NTC] employees with a security clearance of 'Secret' or above will work on the project or have access to DISA information." Neither DISA nor NTC defined the terms "project" or "DISA information," and it later appeared that DISA and NTC understood these terms differently.

The DISA Project work was distinct from the continued development and support of the core commercial product under the licensing contract. With respect to the latter, DoD understood that the core product was supported through regular updates and security patches by uncleared foreign nationals, as it was, by definition, a COTS solution utilized by many different NTC customers.

On September 12, 2008, NTC was engaged as a directed subcontractor under a prime contract between DISA and a Prime Contractor (the "Prime Contractor").

NTC's contract with the Prime Contractor required that "subcontractor personnel performing services" as part of the DISA Project must be "U.S. Citizens with SECRET (including interim SECRET in accordance with the Agreement) or TOP SECRET security clearances." The terms "Project" and "services" were not defined.

In January 2011, the President of the NTC subsidiary performing the DISA contract informed a DISA official and the Prime Contractor that uncleared foreign nationals located in Russia were performing work on the DISA Project. NTC agreed that this was the case but represented to DISA and the Prime Contractor that NTC had been operating according to its understanding of the contract. NTC understood the contract to allow NTC to use uncleared personnel, including foreign nationals performing work outside the United States, to perform offsite work on the DISA Project, provided that NTC's onsite personnel, with security clearances, did not provide its offsite personnel with classified or sensitive, customer-specific information.

In July 2011, the Prime Contractor and NTC agreed upon Software Development Guidelines (the "Guidelines"), which were incorporated into the contract between the Prime Contractor and DISA. The Guidelines were consistent with NTC's understanding of the contract and permitted uncleared personnel, including foreign personnel performing work outside the United States, to support the DISA Project, provided that those foreign personnel were not provided classified or sensitive customer-specific information. Under the Guidelines, work continued to be performed in Russia.

After the NTC software was implemented at DISA, the Offices and DISA determined that ambiguities in the contract documents and different understandings between DISA and its contractors, among other things, had resulted in an unacceptable degradation of the level of

security DISA had intended to achieve. The Offices' investigation determined that the DISA Project code along with other information was stored on an NTC server in Moscow, and there was evidence that, in some instances, uncleared NTC employees located in Russia and Ukraine knew they were customizing and configuring software code for the DISA Project, and knew the military and sensitive nature of the DISN. At the time, there was public notice that communications to and from Russia were subject to the Russian System of Operative-Investigative Measures ("SORM"). Under SORM, the Federal Security Service of the Russian Federation ("FSB") is authorized to collect, analyze, and store both metadata and content that are transmitted or received on Russian networks and servers. Any DISA data and information sent to Russia and/or transferred over Russian networks via NTC servers were subject to these practices and, therefore, there was a risk that the FSB could gather information about the DISN. Accordingly, the United States removed NTC's products from the DISN. The contract between NTC and the Prime Contractor was terminated in June 2013.

###