

October 10, 2014

Ms. Diane Honeycutt  
National Institute of Standards and Technology  
100 Bureau Drive, Stop 8930  
Gaithersburg, MD 20899

Todd P. Blakely  
Attorney  
Direct: 303.863.2979  
tblakely@sheridanross.com

Via Email  
[cyberframework@nist.gov](mailto:cyberframework@nist.gov)

Re: Experience with the Framework for Improving Critical Infrastructure Cybersecurity --  
Request for Information

Dear Ms. Honeycutt:

I am pleased to submit this Response to address question 8(b) in the above-referenced Request for Information.

It seems as though the focus of cyber security is typically on outside individuals, or hackers, attacking a secure system. There is some focus on keeping private information that is on the system from distribution, but there is little attention paid to cyber security threats to a system from an individual who has access to the system, but uses that access in an inappropriate manner.

For example, J.P. Morgan lost billions of dollars based on derivative bets by those within the company.<sup>1</sup> These bets cost J.P. Morgan \$6 billion in losses and at least \$920 million in fines to U.S. and U.K. regulators.<sup>2</sup> Indeed, Jamie Dimon, the CEO of J.P. Morgan, stated in relation to the bets that "in hindsight, the new strategy was flawed, complex, poorly reviewed, poorly executed, and poorly monitored."<sup>3</sup> In another example, the unauthorized deployment of unapproved trading algorithms by insiders also brought down the Knight Capital Group, erasing three-fourths of the company's equity in one day.

Failures of financial institutions have caused worldwide crises that have weakened national economic security and required government intervention. Thus, the Framework should not only focus on cyber security hackers, or unauthorized distribution of personal information, but should also consider inappropriate use of systems by individuals whom have access to the system.

Perhaps a few specific examples might be useful to convey my thoughts.

As a first hypothetical case, it would be completely inappropriate for a single individual to purchase a derivatives contract involving currency futures that could commit the parent

---

<sup>1</sup> Chris Isidore & James O'Toole, *JPMorgan Fined \$920 Million in 'London Whale' Trading Loss*, CNN Money, Sept. 19, 2013, available at <http://money.cnn.com/2013/09/19/investing/jpmorgan-london-whale-fine/index.html>.

<sup>2</sup> *Id.*

<sup>3</sup> Marcy Gordon, *JPMorgan CEO to Testify on \$2B-plus Trading Loss*, AP: The Big Story, Jun. 13, 2012, available at <http://bigstory.ap.org/article/jpmorgan-ceo-testify-2b-plus-trading-loss>.

Ms. Diane Honeycutt  
October 10, 2014  
Page 2

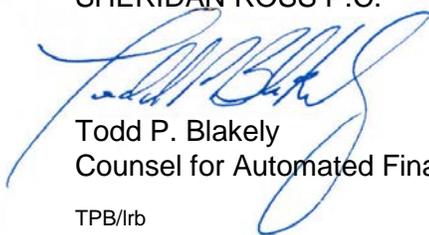
company to a potential \$20 trillion loss. Software and/or hardware can be configured to demand special permission from the CEO of the firm before any such order could be placed electronically. Such a configuration could be called a "Contingency Approval Engine." The "single individual" here can also include a hacker who somehow got unauthorized access to the host computer system. The hypothetical case of a \$20 trillion order could imperil the world's financial system - as did lesser purchases by AIG which preceded the financial catastrophe in 2008. Of course, \$20 trillion is larger than the U.S. GNP. It may also be desirable to demand approval from a governmental oversight board (such as the Federal Reserve) before any such potentially destabilizing order could be placed. It may be helpful to demand that major financial institutions encode their buy orders with an indelible unchangeable code stating the type of transaction (for example, derivative purchase) and the amount (\$20 trillion face value) - to be approved by the use of the Contingent Approval Engine.

As a second hypothetical case, it would be completely inappropriate for any one single individual to send 10 million social security numbers by electronic means to any third party. Software and/or hardware can be configured to demand special permission from the CEO of the firm before any such order could be executed. Such a configuration could also be called a Contingency Approval Engine. The "single individual" here can also include a hacker who got unauthorized access to the host computer system. It may also be desirable to demand approval from a private or governmental oversight board (such as the Financial Services Information Sharing and Analysis Center) before any such potentially harmful order could be executed. The Contingent Approval Engine can be the mechanism used to obtain any such approval.

In these hypothetical cases, the Contingency Approval Engine can be used to prevent potentially world destabilizing financial transactions and can be used to prevent catastrophically harmful data transfers. The Contingency Approval Engine can be configured to act externally to existing computer systems and can be retrofitted to functioning existing computer systems to prevent any disruptions in service. Such approaches may be used to avoid the vulnerability recently demonstrated by Shellshock.

Very truly yours,

SHERIDAN ROSS P.C.



Todd P. Blakely  
Counsel for Automated Financial Oversight Systems, Inc.

TPB/lrb