From:	McGibbon, Gary
To:	regs.comments@federalreserve.gov
Cc:	Morlando, Sal; Romansky, Brian; Mason, Frank; Montanez, Daniel; McKeon, John; McGibbon, Gary
Subject:	12 CFR Chapter II Docket No. OP-1625 - Federal Reserve Board seeks public comment on potential actions to facilitate real-time interbank settlement of faster payments - Request for Comments Due by 12/14/18
Date:	Friday, December 14, 2018 12:33:00 AM
Attachments:	image006.png

NONCONFIDENTIAL // EXTERNAL

Dear Ms. Ann Misback,

Referencing -> https://www.federalreserve.gov/newsevents/pressreleases/other20181003a.htm with comments due by December 14, 2018.

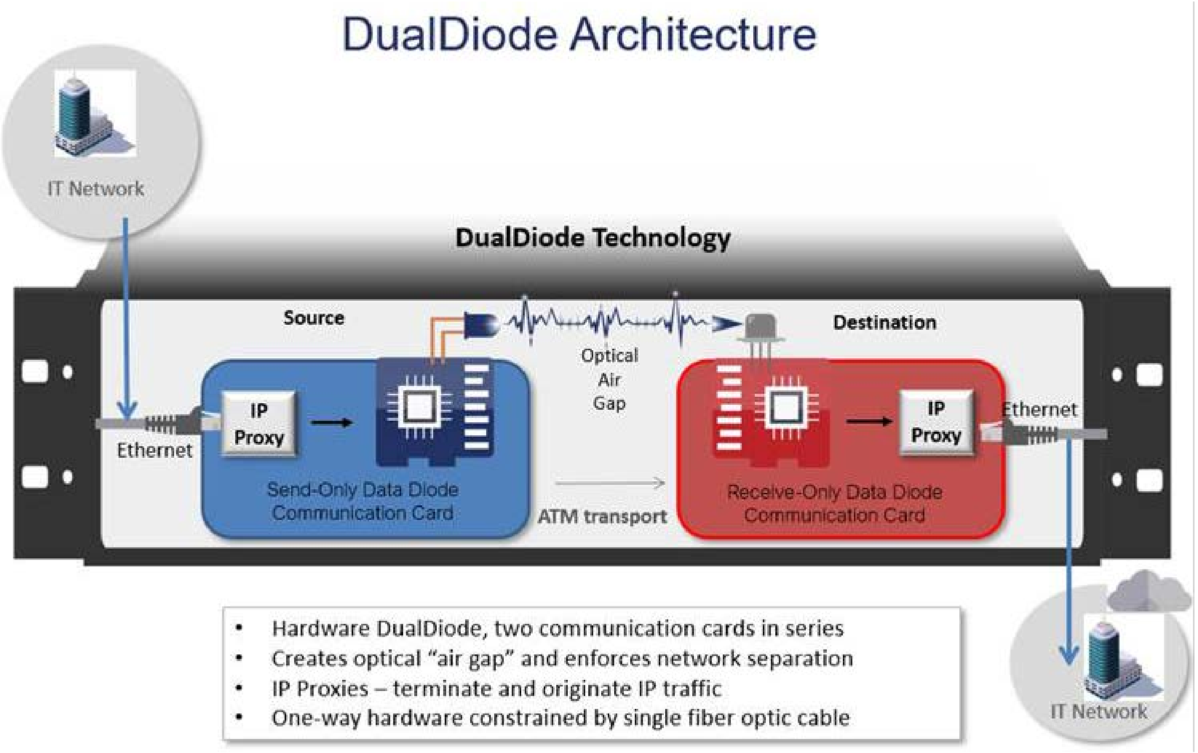
I’d like to offer my comments (my views, not that of, or approved by management at Owl Cyber Defense) on Docket OP-1625 as follows:

As one understands the efforts since enactment of the Federal Reserve Faster Payments Task Force, The Clearing House Payments Company (TCH) has developed a set of message formats for Faster Payments as a Real Time Payments infrastructure. TCH has had this infrastructure in place for a bit over a year. Rather than comment on specifics of the messaging, file formats, and information workflow of such a system, meant to be ubiquitous in the US by 2020, I’d like to offer my comments on the cyber security/ protection of same as follows:

Similar to ACH and Same Day ACH a Real Time Payments/ Real Time Gross Settlement system as to transaction flow, must be absolutely secure. Breaches of the ACH network (Church payroll for $600K, Massachusetts Community College for $800K, etc. due to a weak firewall and up-credentialling) and the SWIFT network ($980M/$80M Central Bank of India, again due to a weak firewall and up-credentialling) have cleared through the Federal Reserve System before they were eventually noticed and intercepted. One could take the position that whatever store and forward file (like SFTP for ACH) or messaging protocol used, utilization of a firewall accessible across the network with vulnerability to exploit through social engineering, east-west movement, up-credentialling and eventually fraud is not the most secure way to segment or ring-fence highly valuable transaction and Personally Identifiable Information (PII) flow through the network. A better, absolutely secure way would be to move the financial information through the store and forward network (with potential content filtering) with a uni-directional cybersecurity gateway or data diode that is deterministic, forward error correcting, self-pacing, low latency, a single box solution that exhibits hardware-enforced one way data flow. In such a solution, a multi-channel, multiprotocol data can be moved between source and destination networks across a virtual air gap with a protocol break ensuring that no routing information is transferred between the two networks, free from external exploit or “phone home” functionality used by criminals to exercise illicit control of data and exfiltration of same.

Similar to the way NIST just finalized a Proof of Concept/ Point of View whitepaper around Privileged Access Management (PAM) with several vendors and demonstrating their interoperability to complete the task at hand, it is believed that the same PoC or lab testbed methodology could be used to demonstrate the full RTP functionality which it is believed, could utilize Owl Cyber Defense's Data Diode products such as the OPDS 100. I've included a screen shot of the Data Diode functionality below and certainly could provide additional information if a testbed were to be built or an end to end solution was captured in a whitepaper.

Please let me know if I can help as the RTP/Faster Payments methodology progresses. Thank You.



DualDiode Architecture

- Hardware DualDiode, two communication cards in series
- Creates optical "air gap" and enforces network separation
- IP Proxies – terminate and originate IP traffic
- One-way hardware constrained by single fiber optic cable

Regards,
Gary McGibbon
Business Development Manager – Financial Services
Owl Cyber Defense Solutions, LLC

+1 919-417-2721 Mobile
+1 203 894 9342 Office

gmcgibbon@OwlCyberDefense.com
www.OwlCyberDefense.com

Winner of Cyber Defense Magazine InfoSec Publisher’s Choice Award – Best Security Hardware Solution