financial institutions to substantial reputation risk. A financial institution should regularly monitor the information it places on social media sites. This monitoring is the direct responsibility of the financial institution, even when such functions may be delegated to third parties. Even if a social media site is owned and maintained by a third party, consumers using the financial institution's part of that site may blame the financial institution for problems that occur on that site, such as uses of their personal information they did not expect or changes to policies that are unclear. The financial institution's ability to control content on a site owned or administered by a third party and to change policies regarding information provided through the site may vary depending on the particular site and the contractual arrangement with the third party. A financial institution should thus weigh these issues against the benefits of using a third party to conduct social media activities.

Privacy Concerns

Even when a financial institution complies with applicable privacy laws in its social media activities, it should consider the potential reaction by the public to any use of consumer information via social media. The financial institution should have procedures to address risks from occurrences such as members of the public posting confidential or sensitive information—for example, account numbers—on the financial institution's social media page or site.

Consumer Complaints and Inquiries

Although a financial institution can take advantage of the public nature of social media to address customer complaints and questions, reputation risks exist when the financial institution does not address consumer questions or complaints in a timely or appropriate manner. Further, the participatory nature of social media can expose a financial institution to reputation risks that may occur when users post critical or inaccurate statements. Compliance risk can also arise when a customer uses social media in an effort to initiate a dispute, such as an error dispute under Regulation E, a billing error under Regulation Z, or a direct dispute about information furnished to a consumer reporting agency under FCRA and its implementing regulations. A financial institution should have monitoring procedures in place to address the potential for these statements or complaints to require further investigation. Some institutions have employed monitoring software to identify any active discussion of the institution on the Internet.

The financial institution should also consider whether, and how, to respond to communications disparaging the financial institution on other parties' social media sites. To properly control these risks, financial institutions should consider the feasibility of monitoring question and complaint forums on social media sites to ensure that such inquiries, complaints, or comments are addressed in a timely and appropriate manner.

Employee Use of Social Media Sites

Financial institutions should be aware that employees' communications via social media—even through employees' own personal social media accounts—may be viewed by the public as reflecting the financial institution's official policies or may otherwise reflect poorly on the financial institution, depending on the form and content of the communications. Employee communications can also subject the financial institution to compliance risk as well as reputation risk. Therefore, financial institutions should establish appropriate policies to address employee participation in social media that implicates the financial institution. The Agencies do not intend this guidance to address any employment law principles that may be relevant to employee use of social media. Each financial institution should evaluate the risks for itself and determine appropriate policies to adopt in light of those risks.

Operational Risk

Operational risk is the risk of loss resulting from inadequate or failed processes, people, or systems. The root cause can be either internal or external events.[33] Operational risk includes the risks posed by a financial institution's use of information technology (IT), which encompasses social media.

The identification, monitoring, and management of IT-related risks are addressed in the *FFIEC Information Technology Examination Handbook,*[34] as well as other supervisory guidance issued by the FFIEC or individual agencies.[35] Depository institutions should pay particular attention to the booklets ''Outsourcing Technology Services'' [36] and ''Information Security'' [37] when using social media, and include social media in existing risk assessment and management programs.

Social media is one of several platforms vulnerable to account takeover and the distribution of malware. A financial institution should ensure that the controls it implements to protect its systems and safeguard customer information from malicious software adequately address social media usage. Financial institutions' incident response protocol regarding a security event, such as a data breach or account takeover, should include social media, as appropriate.

Conclusion

As noted previously, the Agencies recognize that financial institutions are using social media as a tool to generate new business and provide a dynamic environment to interact with consumers. As with any product channel, financial institutions must manage potential risks to the financial institution and consumers by ensuring that their risk management programs provide appropriate oversight and control to address the risk areas discussed within this guidance.

Federal Financial Institutions Examination Council.

Dated: January 17, 2013.

Judith E. Dupre,

FFIEC Executive Secretary.

[FR Doc. 2013–01255 Filed 1–22–13; 8:45 am]

BILLING CODE 7535–01–P; 6210–1–P; 4810–33–P; 4810–AM–P; 6714–01–P

financial/2008/fil08044a.html; NCUA Letter 07–CU–13, *Evaluating Third Party Relationships* (Dec. 2007), *available at http://www.ncua.gov/Resources/Documents/LCU2007-13.pdf*; OCC Bulletin OCC 2001–47, *Third-Party Relationships* (Nov. 1, 2001), *available at http://www.occ.gov/news-issuances/bulletins/2001/bulletin-2001-47.html.*

[33] FFIEC IT Examination Handbook: Management booklet, 2–3 (June 2004), *available at http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_Management.pdf.*

[34] *Available at http://ithandbook.ffiec.gov/it-booklets.aspx.*

[35] FFIEC InfoBase at *http://ithandbook.ffiec.gov.*

[36] *Available at http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_OutsourcingTechnologyServices.pdf.*

[37] *Available at http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf.*

FEDERAL RETIREMENT THRIFT INVESTMENT BOARD

Sunshine Act Meeting

TIME AND DATE: 9:00 a.m. (Eastern Time), January 28, 2013.

PLACE: 10th Floor Board Meeting Room, 77 K Street NE., Washington, DC 20002.

STATUS: Parts will be open to the public and parts will be closed to the public

Matters To Be Considered

1. Approval of the Minutes of the December 17, 2012 Board Member Meeting.
2. Thrift Savings Plan Activity Report by the Acting Executive Director.
a. Monthly Participant Activity Report.
b. Monthly Investment Performance Report.
c. Legislative Report.
3. Quarterly Investment Policy Report.
4. Quarterly Vendor Financials Review.
5. Annual Expense Ratio Report.
6. Annual Statement.
7. 2013 Board Meeting Calendar.

Parts Closed to the Public

8. Personnel.
9. Procurement.
10. Security.
11. Legal.

CONTACT PERSON FOR MORE INFORMATION: Kimberly Weaver, Director, Office of External Affairs, (202) 942–1640.

Dated: January 18, 2013.

James B. Petrick,

Secretary, Federal Retirement Thrift Investment Board.

[FR Doc. 2013–01410 Filed 1–18–13; 4:15 pm]

BILLING CODE 6760–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

Office of the Director, National Institutes of Health; Amended Notice of Meeting

Notice is hereby given of a change in the meeting of the Recombinant DNA Advisory Committee, January 24, 2013, 09:00 a.m. to January 24, 2013, 04:00 p.m., National Institutes of Health, Building 45, 45 Center Drive, Lower Level, Conference Room C1–C2, Rockville, MD, 20892 which was published in the **Federal Register** on January 08, 2013, 78FRN1216.

The time of the meeting has been changed from 9:00 a.m.–4:00 p.m. to 8:30 a.m.–4:30 p.m. Additionally, this meeting will not be webcast and there will be no opportunity to submit comments during the meeting. The meeting is open to the public.

Dated: January 16, 2013.

Carolyn A. Baum,

Program Analyst, Office of Federal Advisory Committee Policy.

[FR Doc. 2013–01231 Filed 1–22–13; 8:45 am]

BILLING CODE 4140–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

Eunice Kennedy Shriver National Institute of Child Health & Human Development; Notice of Closed Meeting

Pursuant to section 10(d) of the Federal Advisory Committee Act, as amended (5 U.S.C. App.), notice is hereby given of the following meeting.

The meeting will be closed to the public in accordance with the provisions set forth in sections 552b(c)(4) and 552b(c)(6), Title 5 U.S.C., as amended. The grant applications and the discussions could disclose confidential trade secrets or commercial property such as patentable material, and personal information concerning individuals associated with the grant applications, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

Name of Committee: National Institute of Child Health and Human Development Special Emphasis Panel; ''Heritable Epigenome.''

Date: February 13, 2013.

Time: 1:00 p.m. to 3:00 p.m.

Agenda: To review and evaluate grant applications.

Place: National Institutes of Health, 6100 Executive Boulevard, Rockville, MD 20852.

Contact Person: Dennis E. Leszczynski, Ph.D., Scientific Review Officer, Division of Scientific Review, National Institute of Child Health and Human Development, NIH, 6100 Executive Blvd., Room 5b01, Bethesda, MD 20892, 301–435–2717, *leszcyd@mail.nih.gov.*

(Catalogue of Federal Domestic Assistance Program Nos. 93.864, Population Research; 93.865, Research for Mothers and Children; 93.929, Center for Medical Rehabilitation Research; 93.209, Contraception and Infertility Loan Repayment Program, National Institutes of Health, HHS)

Dated: January 16, 2013.

Michelle Trout,

Program Analyst, Office of Federal Advisory Committee Policy.

[FR Doc. 2013–01230 Filed 1–22–13; 8:45 am]

BILLING CODE 4140–01–P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

[Docket No. USCG–2009–0973]

Random Drug Testing Rate for Covered Crewmembers

AGENCY: Coast Guard, DHS.

ACTION: Notice of minimum random drug testing rate.

SUMMARY: The Coast Guard has set the calendar year 2013 minimum random drug testing rate at 25 percent of covered crewmembers. The Coast Guard will continue to closely monitor drug test reporting to ensure the quality of the information. The Coast Guard may set the rate back up to 50 percent of covered crewmembers if the positive rate for random drug tests is greater than 1 percent for any one year, or if the quality of data is not sufficient to accurately assess the positive rate.

DATES: The minimum random drug testing rate is effective January 1, 2013, through December 31, 2013. Marine employers must submit their 2013 Management Information System (MIS) reports no later than March 15, 2014.

ADDRESSES: Annual MIS reports may be submitted by mail to Commandant (CG–INV), U.S. Coast Guard Headquarters, 2100 Second Street SW., STOP 7561, Washington, DC 20593–7581 or by electronic submission to the following Internet address: *http://homeport.uscg.mil/Drugtestreports.*

The docket for this notice is available for inspection or copying at the Docket Management Facility (M–30), U.S. Department of Transportation, West Building Ground Floor, Room W12–140, 1200 New Jersey Avenue SE., Washington, DC 20590, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. You may also find this docket on the Internet by going to *http://www.regulations.gov,* inserting USCG–2009–0973 in the ''Search'' box, and then clicking ''Search.''

FOR FURTHER INFORMATION CONTACT: For questions about this notice, please contact Mr. Robert C. Schoening, Drug and Alcohol Program Manager, Office of Investigations and Casualty Analysis (CG–INV), U.S. Coast Guard Headquarters, telephone 202–372–1033. If you have questions on viewing or submitting material to the docket, call Barbara Hairston, Program Manager, Docket Operations, telephone 202–366–9826.

SUPPLEMENTARY INFORMATION: Under 46 CFR 16.230, the Coast Guard requires marine employers to establish random drug testing programs for covered crewmembers. Every marine employer is required by 46 CFR 16.500 to collect and maintain a record of drug testing program data for each calendar year and submit this data by March 15 of the following year to the Coast Guard in an annual Management Information System (MIS) report. Marine employers may either submit their own MIS reports or have a consortium or other employer representative submit the data in a consolidated MIS report.