☐ *Original* ☐ *Amendment*

**U.S. House of Representatives**
**Committee on Ethics**



# EMPLOYEE POST-TRAVEL DISCLOSURE FORM

This form is for disclosing the receipt of travel expenses from private sources for travel taken in connection with official duties. This form does not eliminate the need to report privately-funded travel on the annual Financial Disclosure Statements of those employees required to file them. In accordance with House Rule 25, clause 5, **you must complete this form and file it with the Clerk of the House, 135 Cannon House Office Building, within 15 days after travel is completed**. Please **do not** file this form with the Committee on Ethics.

**NOTE: Willful or knowing misrepresentations on this form may be subject to criminal prosecution pursuant to 18 U.S.C. § 1001.**

1. Name of Traveler: Aaron Hiller

2. a. Name of accompanying relative: _____ ***or*** None ☑
   b. Relationship to Traveler: ☐ Spouse ☐ Child ☐ Other (specify): _____

3. a. Dates of departure and return: Departure: 8/14/17 Return: 8/17/17
   b. Dates at personal expense (if any): _____ ***or*** None ☑

4. Departure city: Boston Destination: San Francisco Return city: Boston

5. Sponsor(s) (who paid for the trip): Stanford University

6. Describe meetings and events attended: Annual cybersecurity conference

7. Attached to this form are EACH of the following (*signify that each item is attached by checking the corresponding box*):
   a. ☐ a completed Sponsor Post-Travel Disclosure Form;
   b. ☑ the Primary Trip Sponsor Form completed by the trip sponsor prior to the trip, including all attachments and Grantmaking or Non-Grantmaking Sponsor Forms;
   c. ☑ page 2 of the completed Traveler Form submitted by the employee; ***and***
   d. ☑ the letter from the Committee on Ethics approving my participation on this trip.

8. a. I represent that I participated in each of the activities reflected in the attached sponsor's agenda. (*Signify that statement is true by checking box*): ☑
   b. If not, explain: _____

I certify that the information contained on this form is true, complete, and correct to the best of my knowledge.

SIGNATURE OF TRAVELER: [signature] DATE: 8/28/17

I authorized this travel in advance. I have determined that all of the expenses listed on the attached Sponsor Post-Travel Disclosure form were necessary and that the travel was in connection with the employee's official duties and would not create the appearance that the employee is using public office for private gain.

NAME OF SUPERVISING MEMBER: John Conyers, Jr. DATE: 8/28/17

SIGNATURE OF SUPERVISING MEMBER: John Conyers Jr.

*Version date 2/2015 by Committee on Ethics*

21

■ *Original* ☐ *Amendment*

**U.S. House of Representatives**
**Committee on Ethics**

# SPONSOR POST-TRAVEL DISCLOSURE FORM

This form must be completed by an officer of any organization that served as the primary trip sponsor in providing travel expenses or reimbursement for travel expenses to House Members, officers, or employees under House Rule 25, clause 5. ***A completed copy of the form must be provided to each House Member, officer, or employee who participated on the trip within 10 days of their return.*** You must answer all questions, and check all boxes, on this form for your submission to comply with House rules and the Committee's travel regulations. Failure to comply with this requirement may result in the denial of future requests to sponsor trips and/or subject the current traveler to disciplinary action or a requirement to repay the trip expenses.

**NOTE: Willful or knowing misrepresentations on this form may be subject to criminal prosecution pursuant to 18 U.S.C. § 1001.**

1. Sponsor(s) (who paid for the trip): Stanford University

2. Travel Destination(s): Stanford University, Palo Alto, CA

3. Date of Departure: 08/14/2017 Date of Return: 08/17/2017

4. Name(s) of Traveler(s): Aaron Hiller
(NOTE: You may list more than one traveler on a form only if all information is identical for each person listed.)

5. **Actual amount** of expenses paid on behalf of, or reimbursed to, each individual named in response to Question 4:

| | Total *Transportation* Expenses | Total *Lodging* Expenses | Total *Meal* Expenses | *Other* Expenses (dollar amount per item and description) |
|---|---|---|---|---|
| Traveler | $494.40 - Flight | $ 450 | $182.50 | $82.63 - Ground Transportation |
| Accompanying Relative | N/A | N/A | N/A | N/A |

6. All expenses connected to the trip were for actual costs incurred and not a *per diem* or lump sum payment. (*Signify statement is true by checking box*): ■

. I certify that the information contained in this form is true, complete, and correct to the best of my knowledge.

Signature: Michael G. Franc

Name: Michael G. Franc Title: Director of Washington D.C. Programs

Organization: Hoover Instituion

**I am an officer of the above-named organization** ***(signify statement is true by checking box)*****:** ■

Address: 1399 New York Avenue NW, Suite 500

Washington D.C. 20005

Telephone number: (202) 760-3200

Email Address: mfranc@stanford.edu

*Committee staff may contact the above-named individual if additional information is required.*

If you have questions regarding your completion of this form, please contact the Committee on Ethics at (202) 225-7103.

**U.S. House of Representatives**
**Committee on Ethics**

**TRAVELER FORM**

1. Name of Traveler: Aaron Hiller

2. Sponsor(s) (who will be paying for the trip): Hoover Institution, Stanford University

3. Travel destination(s): Palo Alto, California

4. a. Date of departure August 14, 2017 Date of return: August 17, 2017
   b. Will you be extending the trip at your personal expense? ☐ Yes ☒ No
   If yes, dates at personal expense: _____

5. a. Will you be accompanied by a relative at the sponsor's expense? ☐ Yes ☒ No
   b. If yes:
   (1) Name of accompanying relative: _____
   (2) Relationship to traveler: ☐ Spouse ☐ Child ☐ Other (specify): _____
   (3) Accompanying relative is at least 18 years of age: ☐ Yes ☐ No

6. a. Did the trip sponsor answer "yes" to Question 9(d) on the Primary Trip Sponsor Form (*i.e.*, travel is sponsored by an entity that employs a registered federal lobbyist or foreign agent and you are requesting lodging for two nights)? ☐ Yes ☒ No
   b. If yes, explain why the second night of lodging is warranted:

7. Primary Trip Sponsor Form is attached, including agenda, invitee list, and any other attachments and contributing sponsor forms: ☒ Yes ☐ No
   NOTE: The agenda should show the traveler's individual schedule, including departure and arrival times and identify the specific events in which the traveler will be participating.

8. Explain why participation in the trip is connected to the traveler's individual official or representational duties. Staff should include their job title and how the activities on the itinerary relate to their duties.

   The annual Cyber Boot Camp turns on key technical, legal, economic, and organizational challenged posed by cyber policy today. These issues are all within my portfolio as Chief Oversight Counsel for HJUD.

9. Is the traveler aware of any registered federal lobbyists or foreign agents involved in planning, organizing, requesting, and/or arranging the trip? ☐ Yes ☒ No

10. **FOR STAFF TRAVELERS:**
    **TO BE COMPLETED BY YOUR EMPLOYING MEMBER:**

**ADVANCED AUTHORIZATION OF EMPLOYEE TRAVEL**

I hereby authorize the individual named above, an employee of the U.S. House of Representatives who works under my direct supervision, to accept expenses for the trip described in this request. I have determined that the above-described travel is in connection with my employee's official duties and that acceptance of these expenses will not create the appearance that the employee is using public office for private gain.

Date: June 12, 2017

John Conyers Jr.
Signature of Employing Member

## U.S. House of Representatives
## Committee on Ethics

# PRIMARY TRIP SPONSOR FORM

This form should be completed by private entities offering to provide travel or reimbursement for travel to House Members, officers, or employees under House Rule 25, clause 5. A completed copy of the form (and any attachments) should be provided to each invited House Member, officer, or employee, who will then forward it to the Committee together with a Traveler Form ***at least 30 days before the start date of the trip***. The trip sponsor should NOT submit the form directly to the Committee. The Committee Web site (ethics.house.gov) provides detailed instructions for filling out the form.

**NOTE: Willful or knowing misrepresentations on this form may be subject to criminal prosecution pursuant to 18 U.S.C. § 1001. Failure to comply with the Committee's Travel Regulations may also lead to the denial of permission to sponsor future trips.**

1. Sponsor (who will be paying for the trip): Stanford University

2. I represent that the trip will not be financed (in whole or in part) by a registered federal lobbyist or foreign agent (*signify that the statement is true by checking box*): ☒

3. *Check only one:* I represent that:
   a. the primary trip sponsor has not accepted from any other source funds intended directly or indirectly to finance any aspect of the trip ☒ ***or***
   b. the trip is arranged without regard to congressional participation and the primary trip sponsor has accepted funds only from entities that will receive a tangible benefit in exchange for those funds ☐ ***or***.
   c. the primary trip sponsor has accepted funds from other source(s) intended directly or indirectly to finance all or part of this trip and has enclosed disclosure forms from each of those entities. ☐
   If "c" is checked, list the names of the additional sponsors: _____

4. Provide names and titles of **ALL** House Members and employees you are inviting. **For each House invitee, provide an explanation of why the individual was invited** (include additional pages if necessary):

   The congressional employees included on the attached list are being invited due to their background and expertise in the policy area to be discussed during the seminars throughout this trip.

5. Is travel being offered to an accompanying relative of the House invitee(s)? ☐ Yes ☒ No

6. Date of departure: 08/14/2017 Date of return: 08/17/2017

7. a. City of departure: Washington, DC
   b. Destination(s): Stanford University, Palo Alto, CA
   c. City of return: Washington, DC

8. I represent that (*check one of the following*):
   a. The sponsor of the trip is an institution of higher education within the meaning of section 101 of the Higher Education Act of 1965: ☒ ***or***
   b. The sponsor of the trip does not retain or employ a registered federal lobbyist or foreign agent: ☐ ***or***
   c. The sponsor employs or retains a registered federal lobbyist or foreign agent, but the trip is for attendance at a one-day event *and* lobbyist/foreign agent involvement in planning, organizing, requesting, or arranging the trip was *de minimis* under the Committee's travel regulations. ☐

9. Check one of the following:
   a. I checked 8(a) or (b) above: ☒
   b. I checked 8(c) above but am not offering any lodging: ☐
   c. I checked 8(c) above and am offering lodging and meals for one night: ☐ ***or***
   d. I checked 8(c) above and am offering lodging and meals for two nights: ☐
   If "d" is checked, explain why the second night of lodging is warranted: _____

10. Attached is a detailed agenda of the activities the House invitees will be participating in during the travel (*i.e.*, an hourly description of planned activities for trip invitees) (*indicate agenda is attached by checking box*): ☒

11. Check one:
    a. I represent that a registered federal lobbyist or foreign agent will not accompany House Members or employees on any segment of the trip (*signify that the statement is true by checking box*): ☐ *or*
    b. N/A – trip sponsor is a U.S. institution of higher education. ☒

12. For **each** sponsor required to submit a sponsor form, describe the sponsor's interest in the subject matter of the trip **and** its role in organizing and/or conducting the trip:

Stanford University's Hoover Institution is the sole sponsor of the trip, and is a research institution that, through its scholars, library, and archives, promotes economic opportunity and prosperity. Its ~~scholars engage with the policy community and by convening a series of meetings at the Stanford~~ University campus, we will be able to include the participation of many distinguished senior fellows in substantive public policy discussions with employees of House Members.

13. *Answer parts a and b. Answer part c if necessary.*
    a. Mode of travel: Air ☒ Rail ☐ Bus ☒ Car ☐ Other ☐ (Specify: _____)
    b. Class of travel: Coach ☒ Business ☐ First ☐ Charter ☐ Other ☐ (Specify: _____)
    c. If travel will be first class or by chartered or private aircraft, explain why such travel is warranted:

14. I represent that the expenditures related to local area travel during the trip will be unrelated to personal or recreational activities of the invitee(s). (*signify that the statement is true by checking box*): ☒

15. I represent that either (*check one of the following*):
    a. The trip involves an event that is arranged or organized *without regard* to congressional participation and that meals provided to congressional participants are similar to those provided to or purchased by other event attendees: ☐ *or*
    b. The trip involves events that are arranged specifically *with regard* to congressional participation: ☒

    If "b" is checked:

    1) Detail the cost per day of meals (approximate cost may be provided): Meals will be planned to comply with the $64 per diem.

    2) Provide reason for selecting the location of the event or trip: The location of the Hoover Institution's headquarters on the Stanford University campus will allow for greater participation by California-based Hoover senior fellows.

16. Name, nightly cost, and reasons for selecting each hotel or other lodging facility:

Hotel name: Schwab Residential Center City: Stanford Cost per night: $150
Reason(s) for selecting: Owned and operated by Stanford. Proximity to the events that comprise the program.

Hotel name: _____ City: _____ Cost per night: _____
Reason(s) for selecting: _____

Hotel name: _____ City: _____ Cost per night: _____
Reason(s) for selecting: _____

17. I represent that all expenses connected to the trip will be for actual costs incurred and not a per diem or lump sum payment. (*signify that the statement is true by checking box*): ☒

18. TOTAL EXPENSES FOR EACH PARTICIPANT:

| ☐ actual amounts<br>☒ good faith estimates | Total *Transportation* Expenses per Participant | Total *Lodging* Expenses per Participant | Total *Meal* Expenses per Participant |
|---|---|---|---|
| For each Member, Officer, or employee | $600 roundtrip airfare | $450 | $192 |
| For each accompanying relative | N/A | N/A | N/A |

| | *Other* Expenses (dollar amount per item) | Identify Specific Nature of "Other" Expenses (*e.g.*, taxi, parking, registration fee, etc.) |
|---|---|---|
| For each Member, Officer, or employee | $200 | Ground transportation |
| For each accompanying relative | N/A | N/A |

**NOTE: Willful or knowing misrepresentations on this form may be subject to criminal prosecution pursuant to 18 U.S.C. § 1001.**

19. Check one:
    a. I certify that I am an officer of the organization listed below. ☐ ***or***
    b. N/A – sponsor is an individual or a U.S. institution of higher education. ☒

20. I certify that I am not a registered federal lobbyist or foreign agent for any sponsor of this trip. ☒

21. I certify by my signature that the information contained in this form is true, complete, and correct to the best of my knowledge.

Signature: Michael G. Franc

Name: Michael G. Franc

Title: Director, Washington, DC Programs

Organization: Hoover Institution

Address: 1399 New York Ave NW, Suite 500, Washington, DC 20005

Telephone number: (202) 760-3200

Email address: mfranc@stanford.edu

If there are any questions regarding this form please contact the Committee at the following address:

Committee on Ethics
U.S. House of Representatives
1015 Longworth House Office Building
Washington, DC 20515
(202) 225-7103 (phone)
(202) 225-7392 (general fax)

ONE HUNDRED FIFTEENTH CONGRESS

# U.S. House of Representatives

COMMITTEE ON ETHICS



1015 Longworth House Office Building
Washington, D.C. 20515-6328
Telephone: (202) 225-7103
Facsimile: (202) 225-7392

August 4, 2017

Mr. Aaron Hiller
Committee on the Judiciary
2035 Rayburn House Office Building
Washington, DC 20515

Dear Mr. Hiller:

Pursuant to House Rule 25, clause 5(d)(2), the Committee on Ethics hereby approves your proposed trip to Palo Alto, California, scheduled for August 14 to 17, 2017, sponsored by Stanford University.

You must complete an Employee Post-Travel Disclosure Form (which your employing Member must also sign) and file it, together with a Sponsor Post-Travel Disclosure Form completed by the trip sponsor, with the Clerk of the House within 15 days after your return from travel. As part of that filing, you are also required to attach a copy of this letter and both the Traveler and Primary Trip Sponsor Forms (including attachments) you previously submitted to the Committee in seeking pre-approval for this trip. If you are required to file an annual Financial Disclosure Statement, you must also report all travel expenses totaling more than $390 from a single source on the "Travel" schedule of your annual Financial Disclosure Statement covering this calendar year. Finally, Travel Regulation § 404(d) also requires you to keep a copy of all request forms and supporting information provided to the Committee for three subsequent Congresses from the date of travel.

If you have any further questions, please contact the Committee's Office of Advice and Education at extension 5-7103.

Sincerely,

Susan W. Brooks
Chairwoman

Theodore E. Deutch
Ranking Member

SWB/TED:smm

**House**

| Last | First |
|---|---|
| Bergin | Moira |
| Burchfield | James |
| Hiller | Aaron |
| Jacobson | Corey |
| Keeley | Joe |
| Matthews | Madeline |
| Lynch | Tim |
| McElivein | Elizabeth |
| Steward | Lindsay |
| Stock | Troy |

Stanford University

Dear Congressional Staff,

On behalf of Hoover Institution fellows Mike Franc, Herb Lin and Amy Zegart, I would like to formally invite you to participate in Stanford's Congressional Cyber Boot Camp, held in Palo Alto, California on **August 14th – 17th, 2017.** The boot camp is a cross-institutional program created by Stanford's Hoover Institution, Center for International Security and Cooperation, and Freeman Spogli Institute for International Studies.

Designed to give select senior congressional staffers a deeper understanding of cybersecurity issues, the boot camp incorporates a broader network of experts from industry and academia to draw upon in the future. You will examine key technical, legal, economic, psychological, and organizational cyber policy challenges, participate in hands on simulations, taught by world renowned faculty, and engage in discussions with Silicon Valley leaders. We have also dedicated time for dialogue and questions that are of particular interest to you.

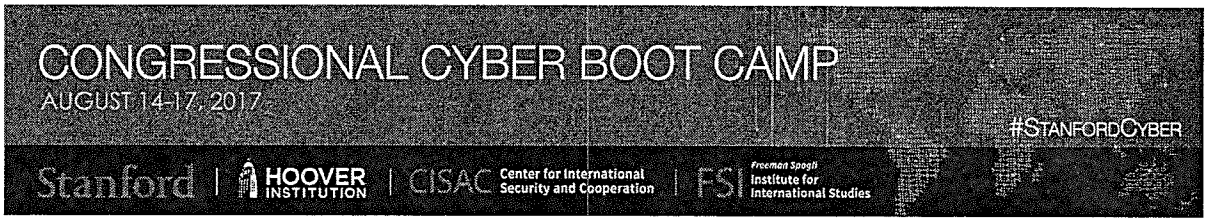
Confirmed speakers this year include: former Secretary of State Condoleezza Rice, former Ambassador to Russia Michael McFaul, former President of Estonia Toomas Hendrik Ilves, co-founder of Andreessen Horowitz, Marc Andreessen, plus many more from academia, tech, and the policy community. A field trip to Tesla's factory and headquarters is also slated on the agenda.

Stanford University will pay for reasonable travel expenses, including round-trip economy airfare, and ground transportation, business class lodging, and meals. The Boot Camp will not be financed in any part by a registered lobbyist or foreign agent, and will comply with all Congressional ethics rules. ***To participate in the Congressional Cyber Boot Camp, please reply to Andrew Clark, afclark@stanford.edu, no later than June 30th.***

We are very much looking forward to your participation and welcoming you to sunny California this August.

Sincere regards,

Russell C. Wald
Senior Manager for External Affairs
Hoover Institution, Stanford University




# SYLLABUS

## FACULTY CO-CHAIRS

**Dr. Amy Zegart**
Co-Director, Center for International Security and Cooperation (CISAC)
Davies Family Senior Fellow, Hoover Institution
Senior Fellow, Freeman Spogli Institute for International Studies (FSI)
Professor of Political Science (by courtesy), Stanford University

**Dr. Herb Lin**
Senior Research Scholar for Cyber Policy and Security, Center for International Security and Cooperation (CISAC)
Hank J. Holland Fellow in Cyber Policy and Security, Hoover Institution
Chief Scientist Emeritus, Computer Science and Telecommunications Board, National Academies

## COURSE DESCRIPTION

Modern nations are increasingly dependent on information and information technology for societal functions. Thus, ensuring the security of information and information technology — cybersecurity — against a broad spectrum of hackers, criminals, terrorists, and state actors is a critical task for the nation. Cybersecurity challenges are evolving at a rapid pace, and the cyber threat the nation faces today will be different from the one it faces tomorrow.

Cybersecurity is not solely a technical matter, although it is easy for policy analysts and others to get lost in the technical details. Improving cybersecurity is a multi-faceted enterprise that requires drawing on knowledge from computer science, economics, law, political science, psychology, and a host of other disciplines. Therefore, this Boot Camp draws upon the expertise of cyber scholars in academia as well as senior business and security professionals in Silicon Valley to provide perspectives on the many dimensions of this dynamic issue.

This Boot Camp will integrate multiple perspectives and disciplines to provide an understanding of the fundamentals of cybersecurity, the nature of cybersecurity threats, various approaches to

addressing these threats, and the use of offensive cyber capabilities to advance national interests. The Stanford Cyber Boot Camp endeavors to give congressional staffers a conceptual framework to understand the threat environment of today and how it might evolve so that they are better able to anticipate and manage the problems of tomorrow.

## Day 1 (Monday, August 14): Cyber Attacks and Responses

**12:00 p.m. – 1:00 p.m.: Lunch & Keynote Address**

**FRAMING THE CYBERSECURITY PROBLEM**

Faculty:

- **Sean Kanuck,** *Former National Intelligence Officer for Cyber Issues, Office of the Director of National Intelligence; CISAC affiliate*

This session will overview the scope of the program (what we cover, what we don't, and why) and set the analytic stage for how we approach the rest of the course.

- Scope: The security implications and challenges of the nation's use of information technology. The course does not address topics such as consumer security, although many concepts covered are relevant.
- Framing Theme #1: Cybersecurity has different meanings and poses different challenges to different stakeholders. Approaching the problem posed requires understanding the perspectives of various actors, their interests, incentives, and organizational demands. Boot Camp sessions are designed to allow staffers to better understand the perspectives of different stakeholders and key players, including attackers and corporate executives.
- Framing Theme #2: The non-technical dimensions of cybersecurity (politics, organizational dynamics, economics, and psychology) are often far more important and less understood than the technical aspects. The Boot Camp pays explicit attention to these non-technical dimensions and how they intersect with technical challenges.
- Framing Theme #3: On the technical side, the course focuses on the underlying foundational principles of computing and communications technology (collectively, information technology) that drive the evolution of architectures, technologies, and vulnerabilities.
- Framing Theme #4: The Boot Camp explains the inherent dominance of offense over defense in cybersecurity and how this fact relates to the "cybersecurity problem."

1:00 p.m. – 2:00 p.m.: Session 1

**THINKING LIKE AN ATTACKER**

Faculty:

- **Peiter Zatko,** *Cyber Independent Testing Lab*
- **Dr. Herb Lin (Discussant),** *Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution*

Effectively combating any adversary requires understanding the ways in which that adversary thinks. Cybersecurity adversaries — from state agents seeking to disable military systems to hacktivists seeking to make a political point — share a security mindset: a predilection for examining the ways in which the security of a system can be circumvented or penetrated. Whereas good engineering is about how a system can be made to work, the security mindset involves thinking about how some aspect of a system can be made to fail. Understanding this mindset is the first step towards designing sound cybersecurity solutions.

Assignment: While in transit to the course location in Palo Alto, conduct a thought experiment for bringing an item prohibited by TSA regulations onto the airplane.

Learning Objectives: Why defense is more difficult than offense and what makes ongoing offense-defense competition inevitable.

2:30 p.m. – 3:30 p.m.: Session 2

**THREATS TO CYBERSECURITY**

Faculty:

- **Carey Nachenberg,** *Google X; Adjunct Assistant Professor of Computer Science, UCLA*

Cybersecurity compromises can take a variety of forms and occur for a variety of reasons. Session 2 examines these compromises and the vulnerabilities in information technology that allow them to happen, again reprising the theme of offensive dominance. This session will include a number of forensic case studies that illuminate the attack spectrum, key challenges, and trends.

Learning Objectives: Security-relevant principles of information technology; types of compromise; the inherent vulnerabilities of information technology; the hidden complexity of cyberspace; anatomy of security compromises; and the spectrum of threats to cybersecurity.

3:45 p.m. – 4:15 p.m.: Keynote Remarks

**THE VIEW FROM EUROPE**

Faculty:

- **Toomas Hendrik Ilves,** *Former President of Estonia; Distinguished Visiting Fellow at CISAC, Hoover, and FSI*

4:30 p.m. – 5:30 p.m.: Dinner & Session 3

**OFFENSIVE DIMENSIONS OF CYBERSECURITY**

Faculty:

- **Jason Healey,** *Senior Research Scholar, Columbia University's School for International and Public Affairs*
- **Dr. Herb Lin,** *Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution*

Offensive activities — including those conducted for espionage and attack purposes —serve a variety of national goals. These goals include, but are not limited to, cyber defense. This discussion will summarize the required strategy, intelligence, and policy necessary for offensive cybersecurity.

Learning Objectives: The role of offensive operations in cyberspace for improving the nation's cybersecurity posture and for other purposes; the differences between attacks and exploitations and the importance of these differences; the scope and nature of U.S. command and control of offensive operations in cyberspace.

6:00 p.m. – 8:30 p.m.: Session 4

## SIMULATION: RESPONDING TO A CYBER CRISIS

Faculty:

- **Michael McNerney,** *Cofounder and CEO of Efflux Systems; CISAC Affiliate*
- **Raj Shah,** *Managing Partner, Defense Innovation Unit Experimental (DIUx)*
- **Joe Sullivan,** *Chief Security Officer, Uber*
- **Ruby Zefo,** *Vice President of the Law & Policy Group and Chief Privacy & Security Counsel, Intel Corporation*
- **Dr. Amy Zegart,** *Co-Director, CISAC; Davies Family Senior Fellow, Hoover Institution; Senior Fellow, FSI*

In this exercise, congressional staffers assume the roles of business executives at a large tech company called Frizzle that has just discovered a major cyber breach. Early forensics indicate that a Frizzle employee opened a malicious PDF file containing a zero-day exploit. This vulnerability enabled the attackers to gain access to F-Net, the company's social networking platform, as well as the Frizzle email user accounts of Chechen activists and sympathizers. In addition, the malicious file may have spread through victims' emails to the Credit Luxe bank in Luxembourg, which processes more than two thirds of Frizzle's user payments. Frizzle's engineering/cybersecurity team, which is one of the best in the world, believes the attack came from Eastern Europe, though much remains unclear.

The CEO has called an emergency meeting of the Board of Directors to formulate a broad-based response to the cyber breach and has asked each of Frizzle's core teams – Engineering / Cybersecurity, Business Strategy, Legal, Public Policy, and Marketing / Communications – to develop and present actionable recommendations to the Board.

The Board of Directors is played by leading Silicon Valley security specialists, lawyers, and entrepreneurs with extensive experience in cybersecurity and business. Board Members attend team breakout sessions and in the "full board meeting" question and discuss each team's recommendations. The simulation concludes with a debrief session where staffers reflect on the simulation and Board Members share insights from their actual experiences confronting cyber challenges.

Learning Objectives: To walk in the shoes of business leaders confronting the early hours and critical decisions of a cyber crisis. Who exactly is hurt or could be hurt by the breach? How could the breach impact Frizzle's business in different markets and its brand reputation? Who are the key stakeholders and how might they react? What actions should Frizzle take and what are the tradeoffs? Should the company "hack back" or publicize the breach to its users, its European bank, its competitors? Work with U.S. government agencies? How do Frizzle's mission and corporate culture guide its response? These are some of the questions staffers will consider.

## Day 2 (Tuesday, August 15): Deep Dive: Technical & Nontechnical Aspects of Cyber

**8:30 a.m. – 10:00 a.m.: Breakfast and Keynote Conversation**

**KEYNOTE** **Conversation with Dr. Condoleezza Rice and Marc Andreessen**

Faculty:

- **Dr. Condoleezza Rice,** *Thomas and Barbara Stephenson Senior Fellow, Hoover Institution; Denning Professor, Stanford Graduate School of Business; former U.S. Secretary of State and National Security Advisor*
- **Marc Andreessen,** *Cofounder and General Partner of Andreessen Horowitz*

**10:15 a.m. – 11:15 a.m.: Session 5**

**FUNDAMENTAL PRINCIPLES OF CYBERSECURITY**

Faculty:

- **Dr. Irving Lachow, Portfolio Manager, International Cyber, MITRE;** *Visiting Fellow, Hoover Institution; Affiliate, CISAC*
- **Dr. John Villasenor,** *Professor of Electrical Engineering, Public Affairs, and Management, UCLA; Vice Chair, World Economic Forum's Global Agenda Council on the Intellectual Property System; Visiting Fellow, Hoover Institution; Affiliate, CISAC*

Although cybersecurity can be a deeply technical subject, especially in how cybersecurity solutions are implemented, a few fundamental principles underlie most solutions. This session takes a deep dive into the fundamental principles of improving cybersecurity and how they fit together. These include reducing reliance on information technology, detecting cybersecurity compromises, and blocking and limiting the impact of compromise. Additional topics include authentication, access control, forensics, recovery, containment, resilience, and active defense.

Learning Objectives: The value of these fundamental principles of cybersecurity and how they can be used collectively to improve security.

11:45 a.m. – 12:45 p.m.: Lunch & Session 6

**ECONOMIC, PSYCHOLOGICAL & ORGANIZATIONAL DIMENSIONS OF CYBERSECURITY**

Faculty:

- **Dr. Dave Clark,** *Senior Research Scientist at the MIT Computer Science and Artificial Intelligence Laboratory*
- **Dr. Tyler Moore,** *Tandy Assistant Professor of Cyber Security and Information Assurance, University of Tulsa*

Known cybersecurity measures are often fully adopted due to a variety of economic, psychological, and organizational factors. These factors are non-technical in nature and often underappreciated by technical and policy communities. Economics describe the incentives that apply to cyber defenders and adversaries, including the nature of cybersecurity market failures and the ability to handle collective action problems. Psychology addresses the deception primary to cybersecurity attacks and the uncertainty of most decision-making in response. An organizational perspective addresses the structural necessities and importance of organizational culture to cybersecurity. This session examines how these factors often discourage the adoption of sound security practices.

Learning Objectives: The importance of economic, organizational, and psychological factors of cybersecurity and why they are often overlooked in efforts to improve cybersecurity; how government action might help to address non-technical factors that diminish the nation's cybersecurity posture.

1:30 p.m. – 2:30 p.m.: Session 7

**DOMESTIC LAW AND INTERNATIONAL LEGAL DIMENSIONS OF CYBER SECURITY**

Faculty:

- **Prof. Matthew Waxman,** *Liviu Librescu Professor of Law, Faculty Chair Roger Hertog Program on Law and National Security, Columbia University*
- **Prof. Robert Chesney,** *Associate Dean and Charles I. Francis Professor, University of Texas School of Law; Director, Robert S. Strauss Center for International Security and Law*

Technological change has far outpaced changes in law and will almost certainly continue to do so in the future. This lag consequentially challenges Congress to craft legislation appropriate for future technology. Furthermore, nations have cooperative and competitive (and sometimes

adversarial) interests that play out in cyberspace. Internet communication does not inherently respect national borders, giving an international dimension to every cybersecurity challenge.

Learning Objectives: For domestic law, the implicit technological assumptions of existing cybersecurity laws; what problems arise in applying existing law to technological circumstances not contemplated at the time of initial passage.

For international dimensions, various legal regimes of potential relevance, including the law of war, human rights law, trade and intellectual property law; proposals for Internet governance; and different non-governmental organizations that affect the design and operation of the Internet.

**2:30 p.m. – 3:00 p.m.**

**DEBRIEF from previous day**

Faculty:

- **Dr. Herb Lin,** *Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution*
- **Dr. Amy Zegart,** *Co-Director, CISAC; Davies Family Senior Fellow, Hoover Institution; Senior Fellow, FSI*

**5:30 p.m. – 8:30 p.m.: Reception & Dinner**

**KEYNOTE** **Conversation between Dr. Michael McFaul and Joel Peterson**

Faculty:

- **Dr. Michael McFaul,** *Director and Senior Fellow, FSI; Peter and Helen Bing Senior Fellow, Hoover Institution, Professor of Political Science, Stanford University; former U.S. Ambassador to the Russian Federation*
- **Joel Peterson,** *Chairman, Jet Blue Airways; Robert L. Joss Adjunct Professor of Management, Stanford Graduate School of Business; Chairman, Hoover Institution Board of Overseers*

## Day 3 (Wednesday, August 16): Civil Liberties, Corporate Interests, and Security

7:45 a.m. – 8:30 a.m.: Breakfast

**DEBRIEF from previous day**

Faculty:

- **Dr. Herb Lin,** *Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution*
- **Dr. Amy Zegart,** *Co-Director, CISAC; Davies Family Senior Fellow, Hoover Institution; Senior Fellow, FSI*

8:30 a.m. – 9:30 a.m.: Session 8

**CYBERSECURITY AND CIVIL LIBERTIES**

Faculty:

- **Anne Neuberger,** *National Security Agency*
- **Jennifer Granick,** *Director of Civil Liberties, Stanford Center for Internet and Society; Affiliate, CISAC; Former Civil Liberties Director, Electronic Frontier Foundation*

Measures intended to support cybersecurity can also threaten certain civil liberties. What cybersecurity means depends in part on whose security is at risk. For some, a threat to civil liberties resulting from greater use of information technology might be interpreted as a cybersecurity threat. Session 8 focuses on this push and pull between security and civil liberties in cyberspace.

Learning Objectives: Different perspectives at the nexus of civil liberties and cybersecurity; how, when, and to what extent, preservation of civil liberties and cybersecurity trade off against one another. Topics to be discussed include privacy, anonymity, and free speech.

9:30 a.m. – 10:30 a.m.: Session 9

**CORPORATE PERSPECTIVES ON CYBERSECURITY**

Faculty:

- **Dr. Sameer Bhalotra (Chair),** *Co-Founder and CEO, StackRox; Senior Associate of the Strategic Technologies Program, CSIS; Affiliate, CISAC; former Senior Director for Cybersecurity, National Security Council*
- **Rick Howard,** *Chief Security Officer at Palo Alto Networks*
- **Matt Miller,** *Partner at Sequoia Capital*

Market forces have a critical role in enhancing or weakening cybersecurity. Session 9 examines how such forces play out at the level of the individual firm and incorporate the views and concerns of the business community. Silicon Valley senior executives and engineers will give their "cyber-ground truths" about the security problems facing the private sector.

Learning Objectives: Various private sector perspectives from technology firms that support innovative efforts for providing IT-based products and services with attention to cybersecurity.

11:00 p.m. – 11:45 p.m.: Session 10

**WHITE HOUSE PERSPECTIVES**

Faculty:

- **Andy Grotto,** *CISAC Perry Fellow; Hoover Research Fellow; Affiliate, CISAC; Former Senior Director for Cybersecurity Policy, National Security Council*

12:00 p.m. – 1:30 p.m.: Lunch Keynote

**DRIVERLESS CARS & PLANE HACKING: SECURITY VULNERABLITIES, CAUSES, AND CHALLENGES**

Faculty:

- **Dr. Stefan Savage,** *Professor of Computer Science and Engineering, UCSD; Director, Center for Network Systems (CNS); Co-Director, Center for Evidence-based Security Research (CESR)*

Modern automobiles are no longer mere mechanical devices; they are pervasively monitored and controlled by dozens of digital computers coordinated via internal vehicular networks. While this transformation has driven major advancements in efficiency and safety, it has also introduced

a range of new potential risks. In 2010, University of California, San Diego and the University of Washington demonstrated the ability to remotely control a popular passenger vehicle with no prior physical access. Recent demonstrations have validated that similar issues exist in other vehicles as well.

Learning Objectives: The nature of automotive security vulnerabilities, the underlying causes, and the challenges (both technical and non-technical) in securing the automotive platform.

**2:30 p.m. – 4:30 p.m.**

**TESLA FACTORY VISIT**

45500 Fremont Blvd, Fremont, CA 94538

**5:30 p.m. – 8:30 p.m.**

**DINNER & FEEDBACK SESSION**

Coupa Café – Stanford Golf Course
198 Junipero Serra Blvd, Stanford, CA, 94305