

# RESEARCH COMPLIANCE

News and Analysis for Colleges, Universities, AMCs and Other Non-Federal Entities

## Contents

- 4** GAO Charts Growth, Consolidation Among 'Independent' Institutional Review Boards
- 5** OIG Investigation? Steps Can Help Your Organization Obtain Best Possible Results
- 9** Research Program Solicitation Could Include Four Topics
- 11** In This Month's E-News



## HCCA®

### Editor

Theresa Defino  
theresa.defino@hcca-info.org

### Copy Editor

Julia Ramirez Burke  
julia.ramirez.burke@hcca-info.org

## JASON Urges NSF to Guard Against Racial, Ethnic Profiling in Research Security Program

If the National Science Foundation (NSF) creates a research program on research security, it should make every effort to ensure the United States remains “the premier destination for top scholars around the world [and] must avoid creating a reputation of racial profiling or injustice,” the independent science advisory group known as JASON concluded in a recent report considering what such a program on research might entail.<sup>1</sup>

“The products of a research program on research security must not be used to disadvantage anyone based on their ethnic background or country of origin,” JASON wrote in the report, in which the NSF asked the group to consider the definition of research security, how that definition might differ from discipline to discipline, what central research themes should be addressed as well as which are most urgent, what critical research communities must be engaged and what data and privacy controls will be required for research on research security.

In the report, released March 30, JASON developed definitions of research security and research integrity to distinguish between the two disciplines. JASON also provided topic areas for a possible NSF program solicitation; it noted that the social sciences will be important for a successful research program on research security.<sup>2</sup>

Overall, JASON found the concept of such a research program to be valuable.

*continued on p. 8*

## When It Comes to Misconduct, Fellows Appeared Uninformed, Unwilling, Hesitant to Report Suspicions

Do you know what research misconduct is, and would you report it if you suspected it?

These deceptively simple questions reflect two pillars of research integrity: recognizing fabrication, falsification and plagiarism (and other untoward practices) and holding those who commit such acts accountable.

Yet more than 200 recipients of National Science Foundation (NSF) graduate research fellowships gave such troubling answers to these and other questions via an anonymous online survey that the authors of a paper deemed them “astonishingly uninformed” and in need of better training that uses real-world examples of unallowable behaviors.

Previous research has “contended that the ultimate responsibility to uncover misconduct rests on individual scientists, and indeed, whistleblowers have been the most common way prominent research fraud cases came to light,” the authors wrote. Yet only 30.7% of 244 fellows surveyed in 2019 said they would report a researcher suspected of misconduct; 60.7% (148) didn’t know if they would.

Additionally, when asked if they had heard of research misconduct in their field in the past five years, across the board, 63% of fellows said they had not, triggering the authors’ “astonishingly uninformed” comment.

*continued*

The open-access paper, “NSF Fellows’ perceptions about incentives, research misconduct, and scientific integrity in STEM [science, technology, engineering and math] academia,” was published April 7 in *Nature Scientific Reports*.<sup>1</sup> It was authored by Siddhartha Roy and Marc A. Edwards. Roy, formerly with the Department of Civil and Environmental Engineering at Virginia Tech, where Edwards is a distinguished professor, is an environmental engineer and research associate at the University of North Carolina-Chapel Hill Water Institute.

Their paper “provides the first ever snapshot of perceptions about academic cheating and research misconduct amongst [a] high-performing group of researchers,” wrote Roy and Edwards, adding “relatively little data” exists about this group and their thoughts on these subjects.

Overall, the responses “cast doubt on the quality and effectiveness of scientific integrity trainings being offered nationwide to engineering graduate students in promoting ethical awareness and behavior,” they wrote.

The survey asked about “cheating, research misconduct, formal integrity training and ethical environments, as well as the overall positives and negatives of academia. NSF’s definition of research misconduct, i.e., the ‘willful fabrication, falsification, plagiarism, and other questionable practices,’ was

displayed before survey respondents answered questions on the topic,” the authors explained.

Responses came from 133 and 111 fellows who had studied civil and environmental engineering or computer science and engineering, respectively—“two broad STEM disciplines that have transformed society but currently face concerns about ethics and high competition for faculty positions,” according to the authors. Interestingly, six (2.5%) fellows “confessed to lying in their survey responses,” and 98 or 40.2% said they were “tempted to lie.”

The group included older and more recent investigators; fellowships were from 2002 to 2007 or 2012 to 2017. Respondents completed the survey from February to May 2019. Additionally, 56.1% (137) were in graduate school at the time, while 43.9% (107) had graduated. A little more than 50% were “employed in academia as graduate students, postdocs or untenured faculty (50.8%) and tenured/tenure-track professors (20.1%).”

### Tenure Pressure, ‘Laziness’ Among Factors

As noted earlier, when asked if they had knowledge of misconduct cases in their field in the past five years, just 89 (36.5%) said yes, and the authors found a significant association between knowledge and “academic stage”—“half of tenured/tenure-track professors ... reported knowledge compared to less than one-third of graduate students or non-tenure track professionals.”

In addition, nine (4%) “confessed to participating in research misconduct,” and 29 (11.9%) “had first-hand knowledge of misconduct by colleagues in their research group, department or field.”

When asked to select “factors that contribute to misconduct or fraud” (more than one choice was allowed), fellows listed the following:

- ◆ “Promotion and tenure pressures” 89%
- ◆ “Funding hyper-competition” 67%
- ◆ “Desire for fame” 56%
- ◆ “Belief in one’s theory” 45%
- ◆ “Laziness” 41%

Other responses indicated that 88.9% of fellows (217) said they “would not engage in misconduct (i.e., fabricate or falsify data) to gain funding, win scholarships or publish in high-impact journals,” another 10.7%, or 26, were “unsure.” The survey also looked at the impact of fellows’ superiors. “If pressured to engage in research misconduct by an advisor,” 7.4% (18) said they would, 37.5% (87) were unsure and 56.9% (139) would not.

**Report on Research Compliance** (ISSN: 1937-6634) is published 12 times a year by Health Care Compliance Association, 6462 City West Parkway, Eden Prairie, MN 55344. 888.580.8373, [hcca-info.org](http://hcca-info.org).

Copyright © 2023 by the Society of Corporate Compliance and Ethics & Health Care Compliance Association. All rights reserved. On an occasional basis, it is okay to copy, fax or email an article from *RRC*. Unless you have HCCA’s permission, it violates federal law to make copies of, fax or email an entire issue; share your subscriber password; or post newsletter content on any website or network. To obtain permission to transmit, make copies or post stories from *RRC* at no charge, please contact customer service at 888.580.8373 or [service@hcca-info.org](mailto:service@hcca-info.org). Contact Halima Omar at [halima.omar@corporatecompliance.org](mailto:halima.omar@corporatecompliance.org) or 952.491.9728 if you’d like to review our reasonable rates for bulk or site licenses that will permit weekly redistributions of entire issues.

**Report on Research Compliance** is published with the understanding that the publisher is not engaged in rendering legal, accounting or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.

Subscriptions to *RRC* include free electronic delivery in addition to the print copy, weekly e-alerts, as well as a searchable database of *RRC* content and archives of past issues at [compliancecosmos.org](http://compliancecosmos.org).

To order an annual subscription to **Report on Research Compliance** (\$425 for HCCA members; \$575 for nonmembers), call 888.580.8373 (major credit cards accepted) or order online at [hcca-info.org](http://hcca-info.org).

**Subscribers to this newsletter can receive 12 non-live Continuing Education Units (CEUs) per year toward certification by the Compliance Certification Board (CCB)<sup>®</sup>. Contact CCB at 888.580.8373.**

The authors cautioned that NSF fellows “are also a group least subject to financial pressures during graduate school due to NSF funding and, therefore, perhaps more likely to accurately describe dominant incentives and external pressures, which may be worse for the typical graduate student.”

Turning to reporting and accountability, the authors found, as noted, only 30.7% “would report another researcher if they suspected misconduct.” Nearly 60% were unsure, and 8.6% said they would not. However, only 4% of those identifying as women said they would not report it.

This possible inaction, the authors wrote, “is probably not surprising given that academics usually have no incentive beyond curiosity, self-interest or a sense of duty to investigate research misconduct.”

In addition, “the repercussions of exposing unethical behavior are potentially catastrophic for whistleblowers, as journal articles, grant applications and awards are anonymously reviewed by peers and severe mental health problems can result from academic shunning and retaliation,” the authors said.

Roy and Edwards also noted that “the incentives for departments and universities where unethical professors bring in large amounts of funding can create conflicts of interest and should be considered.”

### **Often Training Was Online Only**

Is misconduct inevitable? Fellows were split on this question.

Asked to estimate the percentage of researchers who would “succumb to pressure and commit misconduct at least once in their careers,” 5.3% estimated 75% to 100% would, while 61% estimated more than 10% would.

Survey respondents were also asked to identify appropriate punishments for those who commit research misconduct. While they endorsed “public retractions and corrections of the scientific record, firing or revoking of faculty tenure” and “a permanent public record of the misconduct,” only half said research in which the public was harmed should result in “charges or a criminal investigation.” Disagreement about “what constituted distortion of the scientific record” was also evident in the survey answers.

Other questions addressed integrity training; fellows indicated they had attended online sessions, university courses and workshops. Of note, 62.7% participated in online training offered by the Collaborative Institutional Training Institute (CITI). The authors said more than 2,200 institutions offer only CITI training.

The authors called it “concerning” that 54.1% of the surveyed fellows thought their training had no effect on their “ability to handle ethical dilemmas.” Forty-four percent felt more prepared.

Regarding their own behaviors outside of strictly defined research misconduct, 39 (16%) said they had “cheated in college and/or graduate school,” while 205 (84%) said they had not.

Seventy-six (31.1%) reported having “seen their graduate peers cheat.” Copying assignments (81.6%), plagiarism (47.4%) and “using online solutions” (36.8%) were the three most common types of cheating.

“The top two reasons Fellows offered for committing academic cheating or considered a motivation for their peers cheating were good grades (e.g., ‘afraid of bad grades—ashamed of having done so’) and having less time (e.g., ‘felt too busy, had to cut corners to get everything done’). In one department, it was asserted that cheating was the norm (i.e., ‘it [was] unusual if you DON’T have the homework solutions ahead of time’). In another, ‘getting at least the A or B grade [was] required to continue in the program,’” according to the authors.

### **Motivations to Cheat Must Be Understood**

Other reasons cited were “the drive to stay competitive (e.g., ‘I felt that it was a gray area and that I wanted to have a leg up on my classmates’), the advanced nature of graduate-level classes, and preference to do research over classwork (e.g., ‘classes are a waste of time, would rather do research’), were less prominent but still notable factors ... motivating Fellows and their graduate peers to cheat. Altruism (e.g., ‘I was enjoying working with friends and wanted to help them’) was also mentioned.”

More immediate efforts to “reduce cheating and research misconduct ... should consider both individual motivations and academic pressures. Pressure to get promotion/tenure was top-ranked by Fellows as possible motivation behind unethical behavior, which is consistent with recent findings on researcher career stage being a predictive factor for journal retractions that mostly result from scientific misconduct. Integrity training should likely include real world and field-specific case studies and instruction rooted in human nature and organizational psychology,” the authors wrote.

Additionally, they recommended that “educational psychologists, moral psychologists, neuroscientists, behavioral economists and legal scholars” work together to “(a) design ethics training and interventions that reduce occurrence of academic dishonesty and research misconduct, (b) isolate institutional and

field-specific factors that impact motivation and likelihood of misconduct, (c) study the relationship between individual personality traits vis-a-vis academic cheating and misconduct, and (d) formalize and refine conflicts of interest, penalties and reparation processes for misconduct.”

In the longer term, the authors suggested that surveys like theirs should be repeated every 10 years. ✦

#### Endnotes

1. Siddhartha Roy and Marc A. Edwards, “NSF Fellows’ perceptions about incentives, research misconduct, and scientific integrity in STEM academia,” *Scientific Reports* 13, no. 1 (2023): 5701, <https://bit.ly/3L1oghW>.

## GAO Charts Growth, Consolidation Among ‘Independent’ Institutional Review Boards

In 2020, three members of Congress asked the Government Accountability Office (GAO) to investigate institutional review boards (IRBs), alleging “the for-profit model ... creates an inherent conflict of interest” that may be further exacerbated by COVID-19.<sup>1</sup>

Sens. Bernie Sanders, I-Vt., now chair of the Health, Education, Labor and Pensions Committee, Elizabeth Warren, D-Mass., and Sherrod Brown, D-Ohio, told GAO officials their “preliminary investigation” of IRBs “raises questions about whether the commercial IRBs’ reviews of these studies have significant vulnerabilities that may leave patients exposed to unnecessary risks during their participation in clinical trials.”

Nearly three years later, GAO released its report, which more generally poked holes in how both the HHS Office for Human Research Protections (OHRP) and the Food and Drug Administration (FDA) conduct oversight of all kinds of IRBs.<sup>2</sup> A future issue of *RRC* will delve into GAO’s findings and recommendations on this topic and OHRP’s response.

This story provides an overview of details related to the number and type of IRBs that were operational as of April 2021, when GAO conducted its analysis.

### GAO Created ‘Independent’ Label

Somewhat confusingly, GAO divided IRBs into five groups but did not refer to any of them as “commercial” nor identify them by profit status. GAO acknowledged that “neither OHRP nor FDA categorize IRBs in this way.”

Instead, GAO grouped IRBs as “university (which includes colleges and academic medical centers), hospital or health care organization, private, government, and independent.”

GAO defined private IRBs as those “affiliated with private organizations, such as research foundations or businesses that do not provide medical care” and independent as those “not affiliated with organizations that conduct or sponsor research and do not fit one of the [other] categories.”

This approach “involved assigning an IRB to a category based upon the IRB name or address, and by conducting additional research, such as identifying the mission of an organization from its website. We recognize that others attempting such a process might develop different categories and that our approach has limitations,” GAO said, given inconsistencies in FDA and OHRP data, for example, the source of some of the information GAO used.

### Independents Now Review the Most Studies

According to GAO’s analysis, there were 2,303 IRBs operated by 1,780 organizations. In terms of actual numbers, “university-based IRBs are the most prevalent type of IRB that reviewed federally regulated research studies,” it said.

Specifically, the number of each type of IRB and the percent of the total is as follows:

- ◆ University—1,284 (56%)
- ◆ Hospital or health care organization—553 (24%)
- ◆ Private—229 (10%)
- ◆ Government—190 (8%)
- ◆ Independent—47 (2%)

“FDA data show the university-based IRBs reviewed the largest share of studies involving FDA-regulated drugs each calendar year from 2012 through 2020,” GAO said. Despite their small number, independent IRBs were a close second in terms of volume.

“Specifically, in 2020, university-based IRBs reviewed protocols for 48 percent of clinical research conducted under investigational new drug application regulations. In comparison, independent IRBs reviewed research for 41 percent in 2020,” GAO said.

Independents’ market share overtook universities just one year later.

In 2021, “independent IRBs reviewed the largest share of FDA-regulated research (48 percent) compared with other IRB types, with university IRBs reviewing the second-highest share (42 percent). This reflects a trend of independent IRBs reviewing an increasing share of research protocols involving FDA-regulated drugs during the period of our review, from 25 percent in 2012 to 48 percent in 2021,” GAO said.

Using these categories, GAO detailed changes occurring in the IRB market, stating that “two

independent IRBs with private equity backing—WCG and Advarra—illustrate the trend in IRB market consolidation.”

### Two Independents Review 92% of IRB Category Type

Advarra, created in 2017 following the merger of independent IRBs Chesapeake and Schulman Associates, has since purchased three IRBs. Meanwhile, “WCG formed in 2012 from the merger of two independent IRBs—Western and Copernicus Group—and has since acquired four additional IRBs,” according to GAO.

WCG and Advarra “accounted for about 92 percent of the clinical research conducted under investigational new drug applications involving regulated drugs and biologics in 2021 and reviewed by independent IRBs, according to our analysis of FDA data,” GAO said.

GAO cited a number of factors that contributed to independent IRBs’ gains, including the fact that “university research activities grounded to a halt” during the COVID-19 pandemic.

However, its analysis indicated the growth of independent IRBs accelerated sharply beginning in 2016, paralleling a decline in university IRB review volume. Market share of the other types of IRBs has been flat since 2012, according to GAO. ✦

### Endnotes

1. Elizabeth Warren, Sherrod Brown, and Bernie Sanders, “Letter to GAO request on for-profit IRBs,” June 16, 2020, <https://bit.ly/3Lkq6M1>.
2. U.S. Governmental Accountability Office, *Institutional Review Boards: Actions Needed to Improve Federal Oversight and Examine Effectiveness*, January 2023, <https://bit.ly/3ApwTh6>.

## OIG Investigation? Steps Can Help Your Organization Obtain Best Possible Results

Facing an investigation by a federal Office of Inspector General (OIG) can be terrifying for an organization and its employees; however, carefully following a series of action steps can help generate the best outcome possible, two attorneys said.

These steps are “what you need to do and how you should react if the OIG requests documents from your organization, or wants to investigate some potential misconduct, [or] calls in your employees for witness interviews. All of these are scary things. They’re nerve-racking things that cause great anxiety amongst organizations and agencies that are just trying to serve the public, serve their communities, and aren’t used to this type of interaction with an investigative authority,” attorney Mindy Pava—who serves as counsel to the

litigation and investigations, federal grants, health care and education practice groups at Feldesman Tucker Leifer Fidell LLP—said in a webinar.<sup>1</sup>

Fellow attorney Rosie Griffin told webinar attendees there are around 75 OIGs in the federal government, all subordinate to the U.S. Department of Justice (DOJ). The general authorities that OIGs work under are the same, and “structurally, they’re not going to be too different from one another,” she said. OIGs investigate administrative, civil and criminal matters, she said.

Therefore, an investigation doesn’t necessarily indicate that OIG suspects criminal activity, Griffin said. Still, administrative actions can have broad consequences for federal grantees, she pointed out, “So, even within that realm, there are serious consequences, and you want to be handling this interaction correctly from the outset.” She said that the organization should determine whether the attorney handling the matter is from the civil or criminal division because “that’s going to give you an idea right from the start about how the OIG is looking at your matter.” OIG can also coordinate with assistant U.S. attorneys around the country, she said.

HHS’ OIG is the largest in the federal government, and in fiscal year 2022, investigative work led to \$2.73 billion in expected recoveries and 710 criminal actions, Griffin said. OIG investigations led to 736 civil actions and excluded 2,332 individuals and entities from federal health care programs, she added.

Across all OIGs, in fiscal year 2021, OIGs handled more than 1.43 million hotline complaints, closed 17,789 investigations and had 1,058 successful civil actions, Griffin said.

“There is so much OIG activity that even if you think everything is going great, it’s something you should be planning and preparing for because you could wind up being contacted by the OIG whether there’s a ‘there’ there or not.”

### Why Are Organizations Targeted?

OIG investigations arise in many different ways, Griffin said. They include:

- ◆ Whistleblower
- ◆ Audit or site visit discrepancy
- ◆ Major new grant or funding source
- ◆ Ongoing investigations from another agency
- ◆ News reports and other publicly available information
- ◆ Government initiatives such as strike forces
- ◆ Self-disclosure

Self-disclosure almost always sets off an investigation, Griffin said. “It’s a very, very rare place where there’s a self-disclosure, and it just sort of takes care of itself—it’s obvious enough what happened, and the extent of damage is that the government’s just going to accept your word for it. No, they’re going to do their own investigation.”

Investigators are required by law to protect confidentiality, identify themselves in interviews and tell you their purpose, Griffin said. However, they have considerable flexibility in how much they need to tell someone they’re interviewing, she said.

To try and understand what OIG might be looking for, Griffin said there are various questions to ask, including:

- ◆ Is this an investigation, inquiry or examination? Is it administrative, civil or criminal? What is the purpose?
- ◆ Is OIG coordinating with DOJ? If so, is it with a U.S. attorney’s office or with the main department? Is there an assigned assistant U.S. attorney? Is that individual civil, criminal or cross-designated?

### Seek out ‘Breadcrumbs’ of Info

“Guidelines are that agents should share the purpose of their investigation with you to the extent possible,” Griffin said. “They can certainly draw a line there and be, more or less, transparent to you, but it doesn’t hurt to ask, and it’s a good idea to ask early. It’s also in their best interest for you to have a basic understanding of what they’re looking for so that you can get them what they need.”

In situations where the investigator isn’t providing much information, Griffin said, it helps to know how DOJ and its attorneys are involved. “And you can ask, is the FBI involved? That sounds like really bad news, but it’s not necessarily really bad news. I’ve had civil cases where I was representing whistleblowers where FBI agents would be involved in ongoing civil investigations,” due either to close relationships between field offices and the OIG office or because the investigator wants access to special investigative techniques from the FBI.

“These are all kinds of breadcrumbs that you can ask for,” Griffin said. “You may get some answers; you may not. There’s flexibility in how transparent the agents can be with you, but it doesn’t hurt to ask and to keep asking because these things can change.”

It’s possible, for example, that OIG is interviewing witnesses and, in fact, is investigating another organization, she said. It’s also possible that OIG is investigating an entity that passed through grant funds to your organization, she added.

### Agents May Knock on Your Door

OIG investigations can begin in one of two ways: via written requests for information, which include subpoenas, civil investigative demands (CIDs), and other document requests or by unannounced visits from investigators.

Unannounced visits, where agents show up at an organization with no warning, “is probably the most jarring way for things to kick off, but it does happen,” Griffin said.

However, she said, “At the outset, you’re probably going to get a request for documents, primarily to kick things off under CID authority. CIDs work like one-sided discovery where the government is the only party that can ask for anything. So, they can look like document requests. They can look like interrogatories, which are long-form questions that you need to answer back in long form or by producing particular materials or creating particular materials to answer the question.” CIDs also can be used to notice full depositions, Griffin added.

That “first love letter from the government” will most likely ask for broad categories of documents in a specific date range, she said.

“When you receive that mail or when folks show up at the door, time is of the essence,” Griffin said. “It’s really important to carefully read what the investigator has given you. There’s going to be a deadline for production of documents and materials.” She said she almost always contacts the agent or attorney listed on the subpoena or CID and asks for more time to produce the documents because “the timelines provided initially are always really short. The best way to do that is to approach them with a workable plan,” not just a plea for additional time.

Agents are frequently happy to receive a rolling document production as part of an overall plan, she said, adding, “That’s generally acceptable and welcome as long as you keep things clearly organized and you’re communicating regularly, generally through counsel, to manage expectations.”

This process will take “a frustratingly long time,” and organizations need to be prepared for that, Griffin said.

### Legal Hold First Step

Generally speaking, documents will determine how the investigation progresses and can implicate or exonerate an entity, Pava said.

Documents are “the meat of OIG’s investigations,” Pava said. “They want to review your emails, your notes, your meeting minutes. It might be emails from

two or three or four years ago, but they're trying to determine what happened and to piece together what happened through documents. So, this is a really important part of how the OIG conducts its investigation and how you can show, from your entity's point of view, what happened—in a way that hopefully shows that the allegations are unfounded and that you did not have any misconduct."

Pava said organizations should maintain a clear documents and records retention system and follow their policies for recordkeeping. In addition, she said, they should follow best practices in document retention, which include working with information technology (IT) for data organization and assistance, developing a system whereby electronic communications can be retrieved from a central server for a period of several years, enabling access to emails of former employees, setting guidelines on destroying expired data and engaging in clear communications with employees relating to their duties to follow protocol.

"It's important for the high-level people at your organization to know what your document-retention practices are," Pava said. "This is all geared towards making it a much easier and simpler process when you have to review and then produce those documents."

Once OIG serves a subpoena or CID or knocks on the door, the organization needs to enact a litigation hold, also known as a legal hold or a preservation order, Pava said. This involves someone high in the organization sending an email or letter to the employees likely to have the most relevant documents, telling them they must preserve all data related to this potential misconduct. The litigation hold will describe the recipient's obligation and specify what data needs to be preserved, she said.

"If your organization does not inform those people and does not circulate a litigation hold, and then the OIG finds evidence that documents were destroyed, which is called spoliation, the destruction or alteration of potential evidence, that could lead to major ramifications for your organization," Pava said. "So, we want to make sure the legal hold is in place to show the OIG that you are responding to the investigation by taking care of the most relevant documents at issue."

Once the investigation concludes, the legal team or C-suite will send a second notice releasing recipients from the legal hold, Pava said.

### **Selectively Produce Documents**

Searching, preserving and collecting documents is burdensome and expensive, Pava said. Attorneys will develop search terms and date limitations to help identify relevant documents in a custodian's possession,

she said, adding that once the documents are identified, they will be preserved for potential use in the litigation.

The IT department can help identify file types unlikely to contain relevant information, identify centralized sources such as shared servers that may include relevant information, run search terms on a sampling of the data and perform tests to "validate" the terms, Pava said.

If the material in question contains protected health information (PHI), then the organization should communicate with OIG and state that any PHI will be redacted, she said. In addition, documents that are expressly between the organization and its attorney or that show the attorney's work product are protected from disclosure under attorney-client privilege, she said, although there are exceptions.

Organizations should review the subpoena/document request carefully and only produce what is expressly requested, Pava said. In addition, she said, the entity should supply an index of which documents respond to which request; attorneys also recommend "Bates stamping" documents or placing a number on each one, so that document can be referenced easily.

### **Internal Investigation Recommended**

If OIG has contacted an organization, it most likely should conduct its own internal investigation to determine what might have happened, Pava said. In fact, the organization's policies and procedures, or its board, might require an investigation, even though the overall focus of that internal investigation might differ in some ways from OIG investigation, she said.

In many cases, counsel will recommend using the subpoena or document demand as a springboard to conducting an independent internal investigation to uncover the extent of any wrongdoing, Pava said. However, internal investigations can be broader than the OIG subpoena, she added.

The organization will need to decide whether in-house personnel or outside counsel should conduct the investigation, Pava said. Outside counsel will be more expensive, she said, but will eliminate potential conflicts of interest.

Those conducting the internal investigation need to emphasize a culture of confidentiality, especially when employee interviews are taking place, Pava said. "The goal is to get an honest assessment of what caused the misconduct," she said. "So, if employees are gossiping after they're interviewed or trying to get their story straight before they interview, that's a bad thing because then it's much more difficult for the internal investigation to uncover the truth of what happened."

If the internal investigation uncovers additional misconduct, then the organization needs to decide whether to report that to OIG, Pava said. If the internal investigation shows there was criminal conduct, then it's mandatory to disclose it, she said. Otherwise, "the organization has to weigh the pros and cons of disclosure, and sometimes one of the pros is getting a lighter punishment or being able to settle for a smaller amount of money due to cooperating and due to voluntarily disclosing the misconduct."

### Witness Preparation Key

Witness interviews are also part of the OIG investigative process, Pava said, noting that these often produce anxiety among current and former employees. Those being interviewed can expect to be presented with documents—usually emails that they sent or received—and asked to interpret and explain the documents, she said.

Counsel should make it clear to those being interviewed that counsel represents the entity and not the individual witness and that witnesses can consult with personal counsel if they wish, Pava said.

When OIG asks a witness to testify, counsel for the organization can help prepare the witness ahead of time, as long as the witness knows that counsel represents the organization's interest, she said. These prep sessions can involve reviewing documents that OIG will likely use, asking pointed questions to make sure the witness can accurately recount facts and preparing the witness for "legal-style" questions, she said. Prep sessions help cut down on anxiety, she said.

OIG will start the interview by asking witnesses if they did anything to prepare for the interview or met with anyone, and it's perfectly acceptable for the witness to respond that they met with the company's attorney, Pava said. In addition, she said, "I don't know" or "I don't remember" is an acceptable answer to detailed questions, so witnesses should not speculate, she said.

Former employees are under no obligation to testify based on the request to the organization, but OIG can issue a separate subpoena, Pava said. Under those circumstances, she strongly recommended that former employees obtain their own counsel.

Employees should be advised not to talk to OIG agents who attempt to conduct "surprise interviews," Pava said, and instead tell the agent, "If you give me your card, I will have my lawyer contact you."

### Waiting Game: Last Step

Once the organization produces documents and witnesses are interviewed, OIG conducts its analysis, Pava said. There could be "radio silence" for many months, or OIG could ask for additional materials,

she said; in some investigations, there's radio silence between document production and witness interviews.

There's no timeline by which OIG must issue findings, Pava said. Eventually, though, OIG will conclude the investigation, and the organization will receive an answer: "The OIG generally writes a report and determines whether the allegations against your organization are substantiated or unsubstantiated," she said. The report may be published on OIG's website, or information may be included in OIG's semiannual report to Congress, she added.

Findings of potential criminal violations result in a referral to DOJ, Pava said. Allegations that were substantiated but without findings of criminal conduct result in a likelihood of disallowance for the portion of the grant tied to the misconduct, and possible exclusion from federal funding, she said. ✦

### Endnotes

1. Rosie Griffin and Mindy Pava, "OIG Investigations: How to Prepare, Plan, and Respond," webinar, March 7, 2023, <https://bit.ly/3zZhc00>.

## NSF Urged to Guard Against Profiling

*continued from page 1*

"JASON concludes that an NSF research program on research security would be useful in addressing many of the concerns about foreign influence and the security of the US fundamental research ecosystem," the group said. "There are many topics that could be the subject of such a research program and most of these will benefit from strong engagement with social scientists, and collaboration of those social scientists with practicing natural scientists in the fields of interest. Access to data will be a serious challenge to the success of a research program, but one that likely can be mitigated by application of appropriate anonymization methods."

### Research Integrity Versus Research Security

NSF asked JASON to study how, based on current understanding, "research security" can be distinguished from "research integrity" and how to sharpen this distinction. "The concepts of research integrity and research security are intertwined, often in ways that obscure useful and important distinctions," JASON said.

The group offered definitions that it said are closely based on those in the National Science and Technology Council guide for implementation of National Security Presidential Memorandum-33 (NSPM-33). That implementation guidance, released in early 2022, also acknowledged research security challenges as foreign nations—notably China—work to illicitly acquire advanced technologies. But it also said an approach that diminishes America's ability to attract global scientific



talent or that fuels xenophobia against Asian Americans will do real damage.<sup>3</sup>

JASON proposed the following “simpler” definitions for research integrity and research security:

- ◆ Research integrity “is adherence to accepted values and principles—that guide the conduct of research and recognize the expectations of funding agencies, research institutions, and the research community.”
- ◆ Research security “is protecting the means, know-how, and products of research until they are ready to be shared, by approval of the leader(s) of the research program and other stakeholders in their security.”

The definition of research integrity “emphasizes the values and principles that the US and other G7 countries have expressed,” the report said, noting that the six values and principles listed in the definition are from the 2017 report, *Fostering Integrity in Research* by the National Academies of Sciences, Engineering, and Medicine.<sup>4</sup>

“These are broadly shared perspectives in many countries with which the US has longstanding international research collaborations,” the JASON report said. “However, it has become clear, as identified in NSPM-33, that this shared concept is not universally agreed upon. Different countries and cultures may have different views on what are regarded as ethical standards in research, possibly leading to different views on ‘research integrity’ and a different position on what constitutes a breach of research security.”

In addition, the report said, the values listed under “research integrity” are expressed with words that “are quite general and open to interpretation. They do not explicitly mention some of the common values that have been brought to the forefront since 2017. For example, the value of ensuring that research is diverse, equitable, and inclusive, or the value of promoting public trust in the face of growing disinformation. These more specifically stated values are likely to

resonate more with researchers than the general values of fairness and accountability, respectively.”

### ‘Effective’ Education Necessary

In JASON’s definition of research security, research program leaders are seen to be in control of the products of their research and have the primary role in determining what is to be released for publication and public dissemination in other media. “This is often the principal investigator (PI) of the research project,” who also controls the timing of any releases, JASON said.

Still, JASON said the group recognizes that there may be “many stakeholders in the security of the research, and these stakeholders have shared responsibility for such decisions related to various parts of the work. This is particularly evident in large science and technology projects sponsored by federal support at universities, which have offices of research administration and technology transfer. It is essential that there be effective education and training on research security among all of these stakeholders—some of whom are likely already well-versed in the matter—and with all of the working members of research teams.”

JASON suggested that NSF focus on how best to formulate this education and training for domestic and international collaborations as part of its research program on research security.

In addition, in the JASON definition of research security, the group “sought to make clear that the information relevant to research projects includes the means and know-how of research and not just the final products of research.” Distribution of this material “might occur in [traditional publications or on] webpages, social media postings, preprints on ArXiv, bioRxiv, release to the popular press, or others outside the research group,” JASON said.

“This definition implicitly notes that the customs and framework for release of research information are

*continued on p. 11*

## Research Program Solicitation Could Include Four Topics

The JASON report<sup>1</sup> provided four groups of illustrative research topics for a National Science Foundation (NSF) research program on research security, saying that these groups could appear within the format for an NSF Program Solicitation.

These four groups are:

- ◆ **Data collection and analysis.** “One of the key challenges in assessing research security risk has been the lack of relevant data,” JASON said. “Establishing the scale and scope of the research security problem should be an essential ingredient

in an NSF program for research-on-research security.”

NSF could, for example, create a controlled-access data pool of unclassified information for researchers working on this problem, JASON said. This could include case studies of research security breaches; collection and analysis focusing on the frequency and potential severity of security breaches; analysis of how unauthorized transmissions of research results have occurred; analysis of motivations for the premature or

unauthorized transmission of research and how such actions are justified by the individuals involved; analysis of STEM fields that have been of greatest concern and the maturity level of the research when the results were inappropriately transmitted; and comparative assessment of policies of U.S. research institutions and analysis of best practices for research security.

◆ **Risk assessment and quantitative approaches.**

“An area of tension between academic researchers and government agencies is the nature of the risk associated with breaches of research security in fundamental research,” JASON said. “Because the research is ultimately intended for publication in the open literature, it may seem that there is little risk associated with failure to protect such research. However, this ignores damage to the academic enterprise that occurs from unapproved sharing of information from grant proposals under review or manuscripts being considered for publication.”

In addition, some researchers may aim to apply for patent protection, and that effort may be compromised by unapproved release of information, the report said. Overall, JASON said, “the consequences of loss of information are likely to be different in different fields, but in some extreme cases could be severe for economic and/or national security. However, imposing controls that restrict access to research areas could slow progress in critical research areas. Thus, it would be helpful to have reliable models of the effects of different control regimes on the development of research fields.”

◆ **Education and training.** “Breaches of research security and the involvement of foreign governments in such breaches are emerging threats,” JASON said. “Education and training will be required to help the research community understand the nature of the threat and to adopt measures to mitigate it.”

There are significant cultural differences between academics engaged in fundamental research and those who are well-versed in security risks, and those differences will pose a major challenge to the success of this effort, the report said.

“Many academics have regular interactions with foreign faculty, graduate students, and postdocs, and consider these to be critical to their research programs. Law enforcement and intelligence community agencies often lack an understanding of how academic research labs operate with

respect to the relationships among faculty members and the researchers they supervise, and how those interactions differ across scientific disciplines. This problem is exacerbated by the inability to share confidential or classified information with the research community that might help them to understand the risks associated with breaches of research security,” JASON said.

On what the report called “a more hopeful note,” there are already mandated Responsible Conduct of Research training programs, which could be modified to better cover topics of research security, JASON said.

◆ **International cooperation and reduction of threats to research security.** “A major factor in the rise of the US in science and technology has been the nation’s ability to attract and retain talented researchers from around the world,” the report said.

“Many in the academic research community believe that the recent actions taken in the interest of research security have unfairly targeted Asian Americans, and that such actions may cause more damage to our competitiveness than breaches of research security. There are also growing concerns about reciprocity and transparency in international science collaborations, which must be balanced with the reality that, in some disciplines, progress can only be made by continuing to engage in such collaborations,” the report said.

Therefore, JASON said, any NSF research program on research security should include “Assessment of international differences in the views of scientific research integrity and the implications for research security; Analysis of potential costs and benefits to US research security from actively recruiting and retaining students, and faculty from a broader range of countries. Extension of this analysis to underserved regions of the US; Considerations in balancing US interests with global interests and how to mitigate risk when global engagement is essential; [and] Analysis of possible threat reduction strategies and preservation of productive international open science ecosystems.”

**Endnotes**

1. Jane Anderson, “JASON Urges NSF to Guard Against Racial, Ethnic Profiling in Research Security Program,” *Report on Research Compliance* 20, no. 5 (May 2023).

known to the [principal investigator] PI working in the discipline in which the work is done, accounting for differences among disciplines,” the report said. “Interdisciplinary work will inherently require closer attention to such differences.”

Discipline-specific considerations are a significant issue in the definition of research security, given the broad portfolio of research supported by NSF and the increased focus on research areas perceived as relevant to economic and national security, and whether new access restrictions, such as controlled unclassified information categories, should be invoked, JASON said.

JASON concluded that the discipline-agnostic definition the group provided applies to multiple fields “but that the consequences of breaches in research security and the measures to be taken to prevent breaches will differ across disciplines.” For example, ideas in a field such as synthetic biology might be easily reproduced elsewhere because the know-how and capabilities are widespread, while ideas in quantum information science likely are actionable by only a few groups because of the large investment required, the report said.

### **Not First Time JASON Stresses Inclusivity**

This isn’t the first time JASON has urged openness and inclusivity in the face of concerns about inappropriate interference by foreign entities. In December 2019, NSF released a JASON report concluding that “the problem of foreign influence can be met by a combination of more robust research integrity measures, careful consideration of risks before entering into foreign engagements and better information exchange between the [intelligence community], law

enforcement, and academia—all of which are good in any circumstance. We note in particular that expanded expectations with respect to reporting conflicts and commitments would have the strong benefit of making the academic system fairer for all.”<sup>5</sup>

In addition, the new JASON report comes as other federal agencies also grapple with research security. The Office of Science and Technology Policy is seeking public comments on a draft Research Security Programs Standard Requirement developed in response to NSPM-33.<sup>6</sup>

The Standard Requirement calls for research institutions receiving federal science and engineering support in excess of \$50 million per year to establish and operate a research security program that includes elements of cybersecurity, foreign travel security, insider threat awareness and identification, and export control training. The comment period closes on June 5. ✦

### **Endnotes**

1. JASON, *Research Program on Research Security*, March 2023, <https://bit.ly/3MN2wJ1>.
2. Jane Anderson, “Research Program Solicitation Could Include Four Topics,” *Report on Research Compliance* 20, no. 5 (May 2023).
3. Theresa Defino, “OSTP Research Security Guidance Answers Questions, Raises Others,” *Report on Research Compliance* 19, no. 2 (February 2022), <https://bit.ly/43yjk2>.
4. National Academies of Sciences, Engineering, and Medicine, *Fostering Integrity in Research*, 2017, <https://bit.ly/41t70IQ>.
5. Theresa Defino, “JASON Report Suggests Integrity Framework Against Foreign Concerns,” *Report on Research Compliance* 17, no. 1, (January 2020), <https://bit.ly/40dZKzo>.
6. Request for Information; NSPM 33 Research Security Programs Standard Requirement, 88 Fed. Reg. 14,187 (March 7, 2023), <https://bit.ly/3mKd298>.

### **In This Month’s E-News**

◆ **NIH should conduct “site visits to foreign facilities that perform NIH-funded animal research” or require third-party verification to offer “reasonable assurance that award recipients’ annual self-reported project information is reliable and adequate to ensure the humane care and use of laboratory animals,”** according to a new report by the Government Accountability Office (GAO). Without such visits and other new steps, NIH may “miss opportunities to identify and respond to possible instances of noncompliance,” GAO said. NIH agreed with GAO’s recommendation, the only one contained in the report, and also said officials would provide an “action plan” to Congress. GAO noted that in fiscal years 2011 through 2021, NIH used grants or contracts “to obligate roughly \$2.2 billion to about 200 foreign institutions for approximately 1,300

projects involving foreign animal research.” Although funding came from 21 of NIH’s 27 institutes and centers, grants and contracts from three—the National Institute of Allergies and Infectious Diseases, National Cancer Institute and National Institute of Neurological Disorders and Strokes—collectively accounted for 52% of the total. Two-thirds went to research facilities in Canada, Australia and the United Kingdom. (4/20/23)

◆ **The HHS Office of the National Coordinator (ONC) for Health Information Technology issued a proposed rule that “builds on the monumental progress that has been made to support patients and providers across the care continuum,”** according to a blog post by Elise Sweeney Anthony, executive director of the ONC Office of Policy. (4/20/23)

## In This Month's E-News

◆ **The HHS Office of Research Integrity (ORI) concluded that a former assistant professor of medicine at Yale University engaged in research misconduct in research supported by U.S. Public Health Service funds.** ORI found that Carlo Spirli, who had worked in Yale's Department of Digestive Diseases, "engaged in research misconduct by knowingly, intentionally, or recklessly falsifying and/or fabricating data" included in four published papers, two presentations and three grant applications. The data involved "falsified and/or fabricated Western blot image data for cholangiopathies in a murine model of Congenital Hepatic Fibrosis." According to ORI, Spirli reused blot images, with or without manipulating them to conceal their similarities, and falsely relabeled them as data representing different experiments or proteins. Spirli falsified quantitative data in associated graphs purportedly derived from those images in 21 figures included in the papers, presentations and grant applications. (4/13/23)

◆ **The National Science Foundation (NSF) Office of Inspector General (OIG) concluded following an audit that several improvements are needed in NSF's Graduate Research Fellowship Program (GRFP).** Specifically, OIG said NSF did not always ensure that all GRFP reporting and participation requirements were consistently enforced, and NSF did not always supply the information or guidance institutions needed to properly manage awards. "This occurred, in part, because NSF did not have sufficient standard operating procedures for the GRFP or adequately train GRFP staff," the auditors said. "In addition, NSF had insufficient information technology controls to determine award amounts and ensure awards were made only in support of eligible fellows." OIG found that, between 2010 and 2019, "NSF awarded approximately \$824,231 in GRFP funding to institutions in support of fellows the institutions reported had exceeded program limits for time," cost of education allowance and stipend. In addition, the report said that between 2012 and 2019, "NSF awarded more than \$1.2 million to institutions in support of fellows the institutions reported had made unsatisfactory progress or did not submit required activity reports." (4/13/23)

◆ **NSF has issued newly revised questions and answers on how to prepare proposals and administer awards.** The 19-page document, "Frequently Asked Questions (FAQs) On Proposal

Preparation and Award Administration Related to the NSF *Proposal & Award Policies & Procedures Guide* (PAPPG)," includes alphabetical questions on topics ranging from "Assistance Listings (formerly (CFDA Numbers)" to "Uniform Resource Locators (URLs)." (4/6/23)

◆ **The Council on Governmental Relations has published a new report discussing both personal financial and institutional conflict of interest issues where they most commonly occur, including consulting, licensing, and clinical studies.** The report, "Analyzing Personal Financial and Institutional Conflicts of Interest in Academic Research Contexts," also addresses federal research funding agencies' recent focus on the intersection of conflicts and malign foreign influence, including a discussion of recent agency efforts to recast conflicts of commitment as "non-financial conflicts of interest." (4/6/23)

◆ **Allegations of traditional research misconduct and professional misconduct "rose precipitously" over the past five years,** Mike Lauer, NIH deputy director for extramural research, said in releasing new data on total research integrity allegations and NIH's efforts to identify and address integrity issues. In his *Open Mike* blog, Lauer said that NIH "generally handled an average of 100 violations each year up to around 2017." However, the number of violations jumped to 342 in 2018 and rose even further to 549 in 2019, 531 in 2020, 573 in 2021 and 564 in 2022. (3/29/23)

◆ **After reviewing \$1.7 million in expenses claimed by Rensselaer Polytechnic Institute (RPI) for the period between Sept. 9, 2018, and Sept. 10, 2021, auditors for the NSF OIG questioned \$198,137 of costs,** \$116,664 of which was for a service agreement that OIG said was unallowable because it did not benefit the NSF award. In addition, the OIG report said RPI used \$54,492 of participant support funding awarded on two NSF awards to cover nonparticipant expenses, which is not allowable without prior NSF approval. Some of that funding was used to cover faculty summer salaries, employee benefits, overhead and other nonparticipant-related expenses, the OIG report said. In addition, RPI used participant support costs to cover housing, meals and indirect expenses at a conference, even though the grants officer rejected the request to rebudget the participant support costs, the report said. (3/29/23)