


TO: NSPE Board of Directors

cc: NSPE House of Delegates
NSPE Committee, Task Force, Council and Interest Group Chairs
State Society Presidents and Presidents-elect
State Society Executives Council
NSPE Past Presidents

FROM: Mark J. Golden, FASAE, CAE 
Executive Director

DATE: 3 October 2017

RE: Board Update: September 15–30, 2017

With positive feedback from our last update on implementation of the new membership business model, an [Issue 2 update](#) was distributed on September 22 to all state and national leaders to keep you informed. It includes:

- Updates on current implementation activities;
- The deadline and process for requesting tier placement reconsideration and election of integrated/non-integrated affiliation; and
- Listing of integrated state societies to date.

Championing the PE License

Occupational Licensure Update: NSPE continues to lead on ensuring the protection and promotion of engineering licensure. NSPE has been leading a federal-level task force against the growing anti-occupational licensure movement, educating policymakers and the public about the critical need for licensure for a learned profession that, above all else, must protect the public health, safety, and welfare. On September 12, NSPE Government Relations staff participated in a [hearing](#) on occupational licensure, convened by the House Judiciary Committee. In conjunction with the hearing, [NSPE signed onto a letter](#) with state licensing boards and professional associations opposing federal legislation that would undermine states' regulation of occupational licensure. As stated in the letter, "the public is best served when state regulatory boards, duly constituted under state law, are free to make decisions on issues of public health, safety, and welfare." NSPE will continue to proactively engage members of Congress to ensure that engineering licensure is protected in any federal legislation.

Industrial Exemption: A recent [article](#) in the Charleston *Post and Courier* newspaper throws a spotlight on the danger to public safety and the cost to the public of the industrial exemption. According to documents published by the paper, Westinghouse and other contractors used unlicensed engineers to design parts of two unfinished, nuclear reactors in South Carolina, "a potentially criminal shortcut that raises fresh questions about why the multibillion-dollar energy project failed." Westinghouse filed for bankruptcy in March, in part due these failed projects. The story was quickly picked up and shared in NSPE communities.

NSPE encourages states to use the information in this report in newsletters or other updates to their membership to inform members on the activities of NSPE. As a suggestion, it may be most useful to take the bullets of most interest from the transmittal email. The full report (and past reports) can always be found [online](#).

These unfortunate events demand a strong response. Among the actions being considered by NSPE include:

- Contacting the US Nuclear Regulatory Commission requesting a thorough and complete investigation of the events leading up to the failure of the project and seeking an opportunity to testify on the professional engineer's critical role in protecting the public health, safety, and welfare;
- Reaching out to key legislators (including PE members and South Carolina representatives in the US Congress) requesting a congressional investigation of events leading up to the failure at the Columbia site; and
- Continued communication of NSPE's interest, concern, and actions through social media and other communications channels, the NSPE website, and articles in *PE* magazine.

The ramifications of this episode resound beyond the boundaries of any one state, but national will, of course, be working closely with our South Carolina affiliate to ensure a coordinated response, to collaboratively achieve maximum impact.

The PE's Role in Autonomous Vehicles: The second version of the National Highway Traffic Safety Administration's guidance on autonomous vehicles, [A Vision for Safety](#), has reinforced NSPE's disappointment and deepened its concern due to the guidance's failure to adequately address NSPE's expressed public safety concerns.

NSPE has proactively advocated for the need to ensure that major technological, safety, and ethical implications are considered before testing and deploying autonomous vehicles on public roads. NSPE urged NHTSA to revise its initial guidance document, released in 2016, which, while not binding, will play a key role developing and deploying autonomous vehicles. Unfortunately, rather than strengthening the guidelines, this new version explicitly focuses on how to enable manufacturers to accelerate deployment rather than addressing NSPE's critical concerns.

Recognizing the promise of autonomous vehicles, NSPE has been a leading advocate on the need to place the public health, safety, and welfare first, and require a licensed professional engineer to play a key role in the development, testing, and safety certification of autonomous vehicles. NSPE and the professional engineers it represents have a foremost responsibility to protect the public health, safety, and welfare—and to make others aware of ways that safety may be jeopardized. Given the unique technical and ethical expertise that professional engineers possess, NSPE strongly believes professional engineers can play a key role in addressing the ethical and technological challenges raised by autonomous vehicles.

NSPE strongly urges NHTSA to revise its policy to address the following key issues:

There is no requirement for a third-party certification of autonomous vehicles and technologies by someone (i.e., a professional engineer) in the decision chain who has a duty that puts public safety first and overrides competitive pressures. These guidelines allow manufacturers and suppliers to self-certify, eliminating a critical third-party safety check.

- Despite encouraging results of autonomous vehicle deployments in controlled environments, there is still significant work to be done before human-operated and autonomous vehicles can safely share public roads. Many factors—weather, pedestrians, road conditions—are common, rapidly changing, and highly unpredictable. The guidelines assume these hurdles will be easily overcome and do not provide adequate safety protections.
- The enormous ethical implications of deploying autonomous vehicles are simply not addressed. No proposed methods for addressing life-and-death decisions are provided, leaving these critical considerations up to manufacturers. A third-party incorporating the input of all stakeholders should play a key role in this evaluation. These third parties should be legally obligated to place the public health, safety, and welfare above all other considerations.

The risks posed by failing to adequately address public safety protections are too great to ignore. For NHTSA to achieve its mission to “Save lives, prevent injuries, and reduce economic costs due to road traffic crashes, through education, research, safety standards, and enforcement activity,” the recommendations proposed must be incorporated into the next version, slated for release in 2018.

Record-Breaking Advocacy Action Alert: More than 725 NSPE members contacted nearly 300 House offices to oppose a bill that would make sweeping changes to federal motor vehicle safety standards to accelerate the widespread deployment of autonomous vehicles.

The SELF DRIVE Act (H.R. 3388) makes the National Highway Traffic Safety Administration responsible for regulating self-driving cars, preempting state and local standards. Furthermore, the bill would allow automakers to obtain exemptions to deploy up to 25,000 vehicles without meeting existing auto safety standards in the first year, a cap that would rise to 100,000 vehicles annually over three years.

NSPE has been a leading advocate on the need to place the public health, safety, and welfare first, and require a licensed professional engineer to play a key role in the development, testing, and safety certification of autonomous vehicles. This legislation fails to address the major safety, technological, and ethical challenges that must be considered before these vehicles are deployed. NSPE, therefore, urged defeat of the bill.

Unfortunately, the legislation was approved by a voice vote on September 6. The bill will now go to the Senate where separate legislation is being developed. NSPE will continue to proactively advocate for the role of the professional engineer in ensuring the public health, safety, and welfare is of paramount importance in the deployment of autonomous vehicles. Learn more about NSPE’s [Legislative Action Center](#).

New Advocacy Staff Member: I am delighted to introduce NSPE’s new Policy and Advocacy Associate John Keane. John brings a wealth of state legislative and regulatory experience to NSPE. He has already hit the ground running and is quickly coming up to speed on our issues. Please contact John (jkeane@nspe.org) and Arielle Eiser (aeiser@nspe.org) with any state legislative or regulatory issues that we can be of assistance with. We will be continuously working with our state society partners to ensure that the professional engineer is promoted and protected at all levels of government.

Ethical Guide to the Profession

NSPE will be conducting the second of its fall ethics webinars on Wednesday, October 11, 2:00 p.m.-3:00 p.m. Eastern. The course, “Engineering Ethics – [The PE and International and Domestic Gifts](#),” will discuss the obligation of the PE to hold paramount the public health, safety, and welfare and will focus primarily on legal and ethical issues relating to gifts to foreign officials involving US and non-US personnel, as well as gifts to state transportation officials and other ethical and professional practice issues. This webinar is approved for continuing education credit in New York.

Powering Professional Advancement

Design-Build Contracts Explained: New commentary on the 2016 EJCDC¹ Design Build Documents ([D-001](#)) is now available for free to members from the NSPE website. The EJCDC Design-Build Series (D-Series) comprises 18 documents, including this commentary, for use in establishing and administering the contract between a project owner and a design-builder, and for related subcontracts with design professionals, constructors, and advisors.

Looking for a Great Example of Free Publicity? About 12 ½ minutes into the [Nightly Business News](#) on PBS September 21 is a segment on earthquakes. There is a three-second close-up clip of a woman engineer/engineering student performing seismological testing, wearing a hard hat and the navy, green, and blue DiscoverE/National Engineers Week t-shirt at the University of Nevada.

Fellow Nominations Due: It is that time again to begin reminding state/territory leaders that 2018 NSPE Fellow member nominations are due to NSPE by February 1, 2018. All state societies are encouraged to participate in the NSPE Fellow member program by submitting applications for qualified NSPE members. Please be sure to carefully review the criteria and qualifications that are used for selection as there have been some changes made; namely:

1. To be considered for Fellow membership, all nominees must be current NSPE national and state members or Life members.
2. Instructions for completing the nomination form now include a description of what constitutes “involvement in NSPE” and “national service.” Please read these instructions very carefully as this is the most critical information to be included on the nomination form. Nominees must have held at least one elected office at the chapter, state, or national level. It is recommended that the nominee have 10 years or more of active service and involvement at all levels, i.e., national, state, chapter/local.

Instructions and guidance for completing the Fellow nomination form and the nomination form itself can be found [here](#).

¹¹ The Engineers Joint Contract Documents Committee (EJCDC) is a joint venture of NSPE, ASCE and ACEC. It develops, publishes, and updates standard contract documents for the design and construction of engineering projects.

Uniting the PE Community

Is Anyone Following You? NSPE has updated the [Twitter primer](#) for state societies (PDF and Word version are available under “For State Leaders”). Feel free to look it over and let Stacey Ober (sober@nspe.org) know if you have any questions. And, by all means, promote it to your state society volunteers, staff, and chapter leaders who might find it useful.

Also in the works are a second primer focused on “enhancing your Twitter account,” which will cover topics like loading graphics, sharing photos/videos, creating lists, etc., and a third primer covering Facebook, Instagram, and LinkedIn.

The Big Ten: Now available to state societies: “[10 Ways To Improve Member Engagement and Loyalty By Leveraging the NSPE Brand.](#)”

Membership Marketing Update: NSPE membership marketing staff is working on composing drafts of member communications for the new dues model. As part of that effort, NSPE is [requesting that states provide](#) some historical information about dues, and state communication efforts so that marketing messages can be customized to each state society. An [easy online form](#) has been created for you to submit your state’s information.

Supplementary messages on what’s changing and member value are particularly important for the minority of members whose dues will increase under the new model. But even if your state’s dues are staying the same or going down, targeted marketing messages can ensure we are fully and specifically promoting the actual membership value being delivered by both national and the state. This will only increase the effectiveness of recruiting new members and increasing renewals. **Please submit your information no later than October 31.** Please note: Adjustments to timing and messages may be made based on testing and renewal behavior.

We thank you in advance for your participation in this important process!

Membership Calls: Phone calls by national membership staff to all nonrenewing members expiring June 2017 have been completed, and results shared with the State Society Executives Council.

Joining the Brand Family.... Rhode Island, Maryland, and West Virginia have formally adopted new logos for their state societies, bringing the number of state societies included in NSPE family branding to 30.

Services to State Societies: Although implementation of integrated affiliation, approved by the House of Delegates in Atlanta, does not formally occur until membership renewals beginning July 1, 2018, NSPE is already rolling out the services incorporated for state societies in the low-capacity/full-service tier. This includes roll out of the first national-produced, state society [website](#) and generation of the first national-produced state society [newsletter](#) (for the California Society of Professional Engineers). That newsletter mailed September 18. More than 99% were successfully delivered (there were only four bad e-mail addresses, and we will follow up with them to get updated information), and 45% of the recipients opened the newsletter in the first seven days.

Regarding nominations for the position of NSPE vice president, communications have gone out to all HoD delegates; committee, task force, interest group and advisory group

chairs; state society presidents and presidents-elect; and state society executive directors and primary contacts. (The elected individual will serve as vice president in 2018–19, and advance to service as NSPE president in 2020–21.) Nominations must be made in writing, include specified endorsements², and be received no later than January 1, 2018. Please contact Nancy Oswald at 703-684-2856 or noswald@nspe.org if you need further information.

Cybersecurity

Like any other business entity, NSPE is concerned by the increasing frequency and severity of data breaches and other cybersecurity failures that have impacted businesses, large and small, across the globe. Such attacks not only expose the company itself to disruption and even existential threats (such as ransomware attacks), they often expose confidential customer and stakeholder information to hostile actors. As a threshold matter, NSPE is concerned about protecting the confidentiality, reliability, and integrity of its own data and IT systems (internal and in the cloud) and human data management operations. Moreover, although NSPE does *not* possess the most sensitive kinds of customer data (such as social security numbers or financial account information) that an entity like Equifax does, we nonetheless do have a legal, as well as ethical duty, to ensure we are honoring our obligation to protect our members, state societies, NICET certificate holders, and other customers against exposure of their confidential information. As part of this effort, NSPE contracted with Panthera Technologies of Owings Mills, Maryland, to perform penetration testing on both NSPE’s external and internal IT assets. This review was conducted in late July and early August.

The external penetration test mimicked the actions (in a controlled manner) of an actual attacker attempting to exploit weaknesses in network security. By identifying such vulnerabilities, proactive steps can be taken to harden systems against them *before* a breach occurs. Panthera characterizes any vulnerabilities identified in their hacking attempt by severity, from “critical” to “medium.”

The results of the penetration testing performed by Panthera were communicated to NSPE on September 5. Panthera identified five “serious³” potential security threats within NSPE IT systems, and two possible “medium⁴” security threats. The tests found **no** higher order (“critical” or “urgent”) vulnerability threats in NSPE systems.

All five of the “serious” threats were removed from NSPE systems within days of receipt of the report through relatively simple means (generally, implementing available software updates or patches that were missing somewhere in the system). The “medium” threats

² A letter of nomination from the Board of Directors of their State/Territory Society signed by the President or Secretary of the State/Territory Society or a petition of nomination signed by (50) fifty or more NSPE members in good standing. Three letters of recommendation attesting to the effectiveness of the candidate’s leadership abilities are also required.

³ Serious threats are defined as: “Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders.”

⁴ Medium threats may not impact NSPE at all if we are not utilizing those features within our IT systems or if other security measures are in place.

(while more perceived than actual) were also addressed immediately, either through software updates or administrative process improvements⁵.

The outcome of all this external and internal penetration testing to the NSPE IT systems is that we are now much more confident that we don't have any major weaknesses in our IT security; and even if we are attacked, systems are in place to thwart hackers altogether, or at least slow them down enough to dissuade them from continuing the attack and to allow our active cybersecurity measures (both software-based and management-based) time to stop the attack.

Bottom line: Hindsight is 20-20. Cybersecurity weaknesses are often found to have been easily and cheaply preventable after a breach occurs⁶; the challenge is to stay in front of the ever-increasing volume and intensity of cyberattacks before they occur. They are often easy to fix, but only if you find them yourself before the cyber-criminal does. NSPE will remain diligent and proactive in this regard. And while a full-blown, state-of-the-art penetration test by a competent third party may be beyond the means of many of our state partners, we urge you to do what you can to ensure that both software and administrative procedures are kept fully current in all of your own systems.

And remember, you always have access to NSPE leadership resources in the [Leadership Toolbox](#). This includes [talking point](#) scripts and presentations for use by NSPE officers, board members, and other leaders during state visits, chapter meetings, or other venues to promote NSPE and its activities, updated on an at least quarterly basis. Current board members can access an online library of board meeting materials (past, current and future) through the online board book site, ([BoardBookIt](#)).

If you want to review NSPE's history and how that has been translated into current plans with a future-focus, NSPE's purpose, mission, vision and a history of the *Race for Relevance* and the resulting Strategic Plan is summarized in a section called "[Who We Are and What We Do](#)."

⁵ Deficiencies in the care and handling of information by the people who manage a database can be the source of cyber vulnerabilities.

⁶ How many of us, on our home or personal computers and Wi-Fi networks, have antivirus and other security tools installed, but are not as diligent as we know we should be in keeping them fully up-to-date?