Thank you on behalf of The Institute of Internal Auditors for the opportunity to comment on the NICE Framework. Attached is a letter from our CEO and President Richard Chambers. Please let me know if I can be of assistance or if you have any questions. Jill Austin

Jill Austin
Manager, Global Advocacy
Standards and Professional Knowledge
The Institute of Internal Auditors - Global Headquarters

www.theiia.org | www.globaliia.org

The Institute of
Internal Auditors

Richard F. Chambers
Certified Internal Auditor
Qualification in Internal Audit Leadership
Certified Government Auditing Professional
Certification in Control Self-Assessment
Certification in Risk Management Assurance

January 13, 2020

National Initiative for Cybersecurity Education Framework
National Institute of Standards and Technology
100 Bureau Drive, Gaithersburg, MD 20899-2000
Emailed to: nicefr amework@nist.gov

Dear Sir/Madam:

The Institute of Internal Auditors (IIA) thanks the National Institute of Standards and Technology (NIST) for the opportunity to share comments on its National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.

For 78 years, The IIA and its now more than 200,000 internal audit members have aided sound governance and risk-management efforts in public- and private-sector organizations, encouraging strong internal controls and an enterprisewide approach. Auditing information systems and security is top of mind in this age of digital transformation and disruption. We know from The IIA's new annual report *OnRisk 2020* that cybersecurity is the top risk identified by chief audit executives, boards of directors, and C-suite executives.

The IIA recognizes that the NICE Framework is a useful resource for creating guidance and can strengthen an organization's abilities regarding cybersecurity work. With respect to possible improvements in the Framework, we submit that there is an opportunity to incorporate some of the key concepts from the *International Standards for the Professional Practice of Internal Auditing*, the only international standards for the profession of internal auditing.

The IIA *Standards* are relevant to all assurance and advisory engagements, including the audit of cybersecurity. The *Standards*, together with authoritative implementation guidance, represent accepted best practices for all aspects of performing professional audits related to management, planning, delivery, reporting, follow-up, proficiency, due professional care, and the importance of independence and objectivity.

These attributes are uniquely inherent to the internal audit function, commonly referred to as the third line of defense, which differs from management functions (first and second lines of defense) due to its mandate, accountability, positioning, resourcing, and methodology. Further, when a role or task is executed according to these attributes, it allows for a greater level of assurance than what could be achieved by an assessment from an organization's management or second-line functions alone.

There is no recognition in the NICE Framework of the relationships that need to exist between the roles described. We recommend that NIST consider drawing on the principles of the Three Lines of Defense model as a basis for providing useful context and clarification.

There is good opportunity to add to or enhance some of the existing components (the description of specialty areas, roles, tasks, knowledge, skills, and abilities) already included in the NICE Framework, to: 1) make clear the importance of the skill sets referenced above; and 2) call out specific tasks that should be performed by the third line of defense in an independent, objective, systematic, and disciplined manner. These objectives could be also be accomplished by adding specific components to the Framework that refer to internal auditors and internal audit activities as a separate function, as opposed to the generic "audit" term, which could be construed as including duties performed by management functions or functions that report to management.

While not an exhaustive list, the following are examples of modifications that could be considered (edits emphasized in italics):

- **Specialty Areas —** Add a Specialty Area under the "Oversee and Govern" category to specifically call out an independent and objective internal audit function, with direct lines of communication to senior management and boards of directors (when applicable).
- **Work Role OV-PMA-005 "IT Program Auditor" —** modify as follows: "Conducts evaluations of an IT program or its individual components *independently and objectively,* to determine compliance with published standards."
- **Task T0188 —** modify as follows: "*With sufficient planning, proficiency, and due care*, prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions."
- **Task T0188 —** modify as follows: "Review or conduct audits of information technology (IT) programs and projects *with sufficient proficiency and due care."*
- **KSA K0363 —** modify as follows: "*Proficient* knowledge of auditing and logging procedures (including server-based logging)."
- **KSA S0085 —** modify as follows: "*Proficient* skill in conducting audits or reviews of technical systems."
- **KSA S0192 —** modify as follows: "*Proficient* skill in auditing firewalls, perimeters, routers, and intrusion detection systems."

The IIA would be very happy to offer its assistance to your organization to support the process of review and development. The IIA has extensive expertise in this field, and is committed to providing IT guidance under the watchful eye of a panel of experts in IT risks, including the highly respected Global Technology Audit Guide series.

Please do not hesitate to contact The IIA's Managing Director of Global Advocacy, Francis Nicholson, CIA, QIAL, CRMA, at francis.nicholson@theiia.org for any questions or comments.

Best regards,

Richard F. Chambers

Richard F. Chambers, CIA, QIAL, CGAP, CCSA, CRMA
President and Chief Executive Officer
The Institute of Internal Auditors