My name is Cynthia Wright. I am a Principal, Cyber Strategy and Policy for the MITRE Corporation, which supports the US Federal government and its partner nation governments as a Federally Funded R&D Center. I advise partner govs on national cyber strategies, and in particular, on cyber policy and cyber workforce development. The following is my personal feedback based on 25+ years of experience in DoD and national cybersecurity strategy—it is not a formal position of the MITRE Corp or the US Government.

Should AUS prohibit Ransomware payments?

- Yes, from insurers. This will eliminate "deep pockets" expectations by attackers and incentivize organizations to take precautions against Ransomware…which the Commonwealth should help them understand, and potentially fund (consider establishing criteria for gov grants for certain kinds of Ransomware protections based on best practices—criteria might include up-front investment by the org in cybersecurity, or meeting some defined cyber hygiene requirements, and/or financial need combined with societal impact (e.g., hospitals))

- Yes, from organizations, *IF* that organization has not reported the ransomware attack/demand to gov (which should 1) require disclosure to affected customers/clients, 2) keep the attack confidential except for those customers and anonymized information sharing mechanisms

Should the gov require breach reporting?

- Yes, in some cases. Ransomware (see above), cases in which citizen PII is compromised, and where Class 1 systems are affected (where Class 1 is defined as meeting some threshold of national or community criticality)

Should the gov pursue some specific cyber workforce development programs beyond the expansion of STEM curricula?

- Our research suggests that while expanding STEM education and making cyber skills (cross-sector) and cybersecurity an integral part of that education is important, the fastest and most effective way of raising national cyber workforce capacity in the short and medium term is hands-on programs (such as apprenticeships) focused on core cybersecurity skills needed by nearly any organization with a network: how to build, operate, and sustain a basic security stack, maintain situational awareness using configurable and automated tools, and detect/respond to cyber incidents (which may mean escalating to an outside cybersecurity partner). Other skills are associated with SysAdmin and help Desk, and focus on asset awareness/management, identity and access management, and change management (configuration control/updates and patching). These are skills the Aspen Institute has called cyber Middle Skills because they do not require a higher education degree, can be taught in a hands-on environment, and are applicable everywhere.
- These hands-on programs can be created through partnerships between gov and industry, where industry brings its greater resources and "demand signal" to both shape training and attract workers, and government uses its ability to incentivize (through tax policy, grants, public messaging, etc). Some examples are work-study programs offered by industry and academia and

funded in part by government in return for a set period of government service (which need not be immediate); career ladder agreements that provide bonuses, additional opportunities, or other incentives to workers that gain experience in both industry and government at different career phases; and others.

- In addition to the middle skills provided by such programs, certain employers and gov will need higher-end skills such as forensics, reverse engineering, digital evidence handling, etc.—these can be taught in specific programs unique to those employers
- Emphasis on program accessibility is also both important. Accessibility means programs that are affordable, offered outside normal work hours and/or on-line, reachable by public transportation, etc.
- It is important to appeal specifically to women--they tend to make up the largest untapped resource in technical fields and cyber offers a unique opportunity to attract them. Whereas cyber is often perceived as geeky, math-y, coding-focused, and exclusive, programs that emphasize “cyber for what” are often more effective in attracting girls and women than “cyber for cyber’s sake”—that is, are focused on specific problems in various fields like medicine, social benefit, finance, sales/marketing, climate science, etc (every industry has cyber applications—any industry or issue that women/girls are interested in has cyber-related aspects that can offer the “wedge” that gets women and girls interested in cyber and cybersecurity).