FARMER MAC

1999 K Street, N.W., 4th Floor · Washington, DC 20006 · Phone: 800.879.3276 · Fax: 202.872.7713

September 26, 2022

Submitted via email to reg-comm@fca.gov
Autumn R. Agans
Deputy Director, Office of Regulatory Policy
Farm Credit Administration
1501 Farm Credit Drive
McLean, Virginia 22102-5090

Re: Proposed Rule – 12 CFR Part 609 – RIN 3052-AD53 – Document Number 2022-15747; *Cyber Risk Management*; 87 Federal Register 45,281-45,284 (July 28, 2022)

Dear Ms. Agans:

The Federal Agricultural Mortgage Corporation (Farmer Mac or we) is pleased to have this opportunity to respond to the request for public comment on the referenced proposed rule (Proposed Rule) of the Farm Credit Administration (FCA) on Cyber Risk Management. Overall, we support many aspects of the Proposed Rule, which codifies expectations about the responsibility of Farm Credit System institutions to operate under a comprehensive cyber risk framework. But, as discussed in more detail below, we believe that some aspects of the Proposed Rule are overly prescriptive and would be impractical to implement as proposed. Indeed, some of the proposed requirements appear to contradict FCA's stated goals of maintaining "maximum flexibility" for regulated institutions and ensuring the implementation of cyber risk management strategies and practices consistent with industry standards and within the unique risk appetite and tolerance of each organization.

Developing Cyber Security Rules and Regulations

With the increasing global reliance on information technology and attendant evolving and growing cyber risks, we support FCA's efforts to modernize the regulatory guidance for cybersecurity risk management. Farmer Mac recognizes the critical importance of uninterrupted system access, information security, and reliability of information technology to its operational and reputational risk profiles; to deliver on its mission; and to safeguard stakeholder data. To accomplish these goals, we have made substantial financial and human capital investment in our cybersecurity program, enhanced risk management practices, and internal control systems. And, as a New York Stock Exchange listed company and Securities and Exchange Commission (SEC) registered company, we will also be subject to new rules and regulations being developed for public companies for cyber risk management. These are expected to include more specific requirements about disclosing material cyber incidents, as well as developing comprehensive cyber risk assessments, cyber incident plans, and enhanced governance, internal controls, and procedures to mitigate cyber risk and manage information security.

Following the SolarWinds and the Colonial Pipeline cyberattacks, multiple government agencies issued new cybersecurity guidance, directives, and regulations for the financial sector.[1] On March 9, 2022, the SEC proposed rules on cybersecurity risk management, strategy, governance, and incident disclosure for public companies (87 Fed. Reg. 13,524), which require current and follow-up periodic reporting of material cybersecurity incidents (SEC Proposed Cyber Rule). The SEC Proposed Cyber Rule also requires "periodic disclosures about a registrant's policies and procedures to identify and manage cybersecurity risks, management's role in implementing cybersecurity policies and procedures, and the board of directors' cybersecurity expertise, if any, and its oversight of cybersecurity risk."

Several government-affiliated groups, including the Federal Financial Institutions Examination Council (FFIEC), which FCA has been consulting with, have been working to develop cyber security best practices, regulatory guidance, and frameworks for the last decade. The FFIEC has developed its Cybersecurity Assessment Tool (CAT) to assess and measure institutions' cybersecurity preparedness. The CAT consists of two parts: an Inherent Risk Profile to determine an institution's inherent risk before implementing controls; and a Cybersecurity Maturity assessment to identify specific controls and practices that are in place. The FFIEC determined that there is no uniform one-size-fits-all methodology to addressing the unique cybersecurity risk profiles of each institution. The FFIEC created the CAT to provide comprehensive assessment of the inherent risks of the institution and security measures in place to best understand and manage the unique cyber risks of the organization. The National Institute of Standards and Technology of the U.S. Department of Commerce (NIST) has engaged vigorously with stakeholders to set priorities and develop a Cybersecurity Framework (CSF) of standards, guidelines, and best practices. CSF creates unique profiles of an organization's alignment of its business requirements and objectives, risk appetite, and resources to identify the feasible best practices to reduce organizational cybersecurity risk levels. NIST initially produced the CSF in 2014, updated it in 2018, and is planning a new, significant update to the CSF in response to advances in technologies and the ever-increasing cybersecurity challenges faced by stakeholders.

---

[1] In late 2021, the Federal Trade Commission (FTC), the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve (FRB), and the Federal Deposit Insurance Corporation (FDIC) promulgated final rules on cybersecurity requirements for the financial services sector. The FTC amended the Gramm-Leach-Bliley Act Safeguards Rule to require FTC-regulated financial institutions to develop comprehensive information security programs and implement cybersecurity requirements (86 Fed. Reg. 70,272 (12/21)). The OCC, FRB, and FDIC implemented rules requiring regulated banks to notify regulators of a computer-security incident that has materially disrupted or degraded a banking organization's ability to carry out banking operations, activities, or processes that would pose a threat to the financial stability of the United States (86 Fed. Reg. 66,424 (11/21)).

The FFIEC and NIST have developed best practices and regulatory guidance based on a risk-based case-by-case assessment of the cyber risks faced by an organization and its cybersecurity program. In line with this, we believe that the Proposed Rule should reflect and be grounded in a similar dynamic, principles-based cyber risk framework. One of FCA's expressed goals in the Proposed Rule is to maintain maximum flexibility for regulated institutions, recognizing their varying degrees of size and complexity. In furtherance of this goal and in light of the most recent industry guidance, best practices, and frameworks developed in recent years by FFIEC, NIST, and the other government agencies and cybersecurity industry experts, we suggest that the Proposed Rule should be revised to be less prescriptive to focus on the unique cybersecurity risks of each regulated organization. That approach would permit each regulated institution to identify and manage risk specific to its particular information security requirements, vulnerabilities, and risk appetite.

With this background in mind, Farmer Mac has comments on the following six areas of the Proposed Rule:

1. Proposed Section 609.930(a): Cyber risk management program.

Farmer Mac agrees with the first sentence of proposed Section 609.930(a) that the institutions regulated by FCA should be required to implement a comprehensive, written cyber risk management program consistent with the size and complexity of the institution's operations. The last sentence of proposed Section 609.930(a),[2] however, raises two issues that Farmer Mac believes should be clarified in any final rule. First, the **"must ensure"** requirement for an institution's cyber risk management program related to the security and confidentiality of information creates a standard that is unattainable in most cases, as a loss of any information provided by a third party, no matter how insignificant, would appear to be a violation of the Proposed Rule as drafted. Farmer Mac suggests that this language be revised to require that the program "**must be designed to protect**" the security and confidentiality of information.

Second, Farmer Mac believes that the reference to **"current, former, and potential customer and employee information"** that must be protected is overbroad without any definition of "customer" or any limitation related to the type or significance of the information provided. Unlike many other institutions regulated by the FCA, Farmer Mac's direct customers are

[2] "The program **must ensure the security and confidentiality of current, former, and potential customer and employee information**, protect against reasonably anticipated cyber threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information." Proposed Section 609.930(a) (emphasis added).

primarily other financial institutions rather than rural borrowers, who are the likely intended beneficiaries of the proposed protections. Farmer Mac safeguards any sensitive borrower information it receives consistent with applicable law and industry standards. It should be noted, however, that not all borrower-related information has the same level of sensitivity and need for protection (some may even be publicly available information) and that once Farmer Mac purchases a loan from a customer (loan seller), the information related to that loan becomes Farmer Mac's rather than the customer's. For example, Farmer Mac does not believe that it should necessarily be required to protect, at pain of a regulatory violation, the non-sensitive information provided by a "potential customer" lender through Farmer Mac's website in the course of exploring Farmer Mac's products and programs. Accordingly, Farmer Mac suggests that FCA clarify what is meant by "customers" and apply the intended protections to only a limited universe of confidential or sensitive personal information.

2. Proposed Section 609.930(b): Role of the board and management.

Farmer Mac supports FCA's goal to provide guidance for effective cybersecurity oversight and to define the respective roles of board and management in managing cyber risk.[3] Although the heading of this section includes a reference to the role of management, the related text of the Proposed Rule does not appear to contemplate a defined role for management even though management's role in managing cyber risk is significant at most organizations. In Farmer Mac's experience, many of the responsibilities assigned to an institution's board of directors in the Proposed Rule are in practice led by members of management. Given the complexity of information security systems and ever-shifting daily cyber risk environments, Farmer Mac believes that the development of the cyber risk program, day-to-day oversight of the company's information security systems, implementation of programs and procedures, and determination of expertise and resource allocation is most appropriately led by members of management with deep information technology expertise.

This is not to say that a board of directors should not provide appropriate oversight of management in developing, implementing, and maintaining a cyber risk program consistent with the board's fiduciary duties and oversight obligations. Even in the absence of an existing applicable regulation on cyber risk management, Farmer Mac's board of directors is keenly

[3] The Proposed Rule in Section 609.930(b) requires the board or an appropriate committee of the board to: (1) approve the written cyber risk program; (2) oversee the development, implementation, and maintenance of the program; and (3) assign roles and responsibilities and determine necessary expertise of the institution's board, management, and employees.

aware of its fiduciary duties to provide effective oversight of the company's cyber risk management program. One way that the board fulfills these fiduciary duties is to ensure that management regularly presents relevant and actionable information about Farmer Mac's cybersecurity program to the Board Enterprise Risk Committee. Those reports include assessments of current and potential cyber risks and any actual incidents, presentations by cyber experts, information requested by the committee on a variety of topics,[4] and management's recommendations for the committee's consideration.

The SEC Proposed Cyber Rule includes an outline of enhanced cybersecurity responsibilities for public company boards of directors and management. In response, public company advisors with expertise in advising boards of directors have weighed in on the appropriate allocation of management responsibilities and board oversight over a company cybersecurity program.[5] Many commenters to the SEC Proposed Cyber Rule observe that the role of a board of directors is to oversee and regularly review, question, and critique the adequacy and effectiveness of management's regular cyber risk assessments, cybersecurity programs, and institution-wide comprehensive management of cyber risk. Those commenters note that management has the technical expertise and daily exposure to the company cyber risks and is therefore best positioned to have the primary responsibility to design, implement, and manage a dynamic comprehensive cyber risk program.

Farmer Mac recommends that Section 609.930(b) of the Proposed Rule be changed not only to better reflect the appropriate roles of the board and management in practice, but also to provide boards with the flexibility to decide which aspects of an organization's cyber risk program may be delegated to management. Farmer Mac's Board Enterprise Risk Committee has the responsibility to provide wide-ranging oversight over Farmer Mac's cyber security program. Management provides, at minimum, quarterly comprehensive reports to the board on the cyber risk management program. Farmer Mac's board of directors has spent a significant amount of time and resources to educate itself about cyber risk management and related

---

[4] For example, Farmer Mac's Enterprise Risk Committee regularly reviews detailed information about: potential enhancements to Farmer Mac's cyber risk program and related policies, internal controls, training, or technology; Farmer Mac's public disclosures about cyber risk; Farmer Mac's incident response plan; results of penetration testing and external assessments; the cyber security posture of key service providers; cyber liability insurance coverage; and the adequacy of corporate resources dedicated to cyber risk management.

[5] See, e.g., RSM "Cybersecurity governance and the board's role" https://rsmus.com/insights/services/risk-fraud-cybersecurity/cybersecurity-governance-and-the-boards-role.html.

industry best practices. Based on that process, the board has adopted the recommended "three lines of defense" approach to managing Farmer Mac's cyber risk. Our chief information security officer function is located within the independent enterprise risk function (second line of defense) rather than within the information technology function (first line of defense) and is also separate from internal and external auditors (third line of defense). Under that approach, the board has in practice delegated to management the responsibility to draft and periodically update the company's written cyber risk program (609.930(b)(1)), as well as to manage the day-to-day operation of the cyber security function, to develop, implement, and maintain the program (609.930(b)(2)), and to assign roles and responsibilities and determine necessary expertise for Farmer Mac's management and employees (609.930(b)(3)).

3. *Proposed Section 609.930(c)(3)(iv): Notifying the institution's board of directors when the institution learns of an incident involving unauthorized access to or use of sensitive or confidential customer and/or employee information.*

Farmer Mac supports the Proposed Rule's requirement to maintain an incident response plan that contains procedures the institution follows when it suspects or detects unauthorized access to sensitive or confidential information (Section 609.930(c)(3)). Farmer Mac has spent significant resources developing its cyber security program with input from outside experts. In the event of a cyber incident, our incident response plan details real-time response protocols involving in-house information technology professionals and outside subject matter experts (if appropriate). Section 609.930(c)(3)(iv) of the Proposed Rule would require notification to the board when there is a cyber incident "involving unauthorized access to or use of sensitive or confidential customer and/or employee information." Our incident response plan, including an incident escalation matrix and board notification thresholds, was recently presented to the Board Enterprise Risk Committee. That committee agreed with management's proposed escalation and notification protocols, which are fundamentally driven by the scope and severity of the security incident. The purpose of an incident escalation matrix is to provide our management and board with a clear and specific action plan in the event of a cyber incident and to delineate the security incidents and risks that are significant enough to be brought to the attention of the board and/or other stakeholders (e.g., regulators and law enforcement). Our incident escalation matrix would categorize a variety of potential cyber incidents involving unauthorized access to sensitive or confidential customer or employee information as not significant enough to require immediate board notification, assuming limited scope, containment, and resolution of the incident. Farmer Mac suggests that Section 609.930(c)(3)(iv) of the Proposed Rule be modified to permit each organization's board of directors to determine for itself when it should be

notified by management of a cyber incident, consistent with the board notification protocols in an organization's approved incident response plan.[6]

4. *Proposed Section 609.930(c)(3)(v): Notifying FCA as soon as possible or no later than 36 hours after the institution determines that an incident has occurred.*

Farmer Mac agrees that FCA's final rule on Cyber Risk Management should require notification to FCA in the event of a cyber incident that presents a potential significant risk to Farmer Mac's continuing business operations or safety and soundness. But the proposed 36-hour deadline to notify FCA of "an incident"[7] in proposed Section 609.930(c)(3)(v) is an unnecessarily tight timeline and over-broad set of incidents requiring immediate notification given the potential scope and frequency of cyber incidents and the time required to internally assess and respond to these incidents. Under our incident response plan, we immediately begin to review and assess any potential cyber incident to determine the scope and severity of the incident and to determine an appropriate action plan to address any attendant cyber risks. This process can require significant technical review of information technology systems and data, and in some cases consultation with third party data security specialists. A systematic review of a cyber incident is likely to take more than 36 hours to marshal the internal and, in some cases, external resources to gather and analyze the data when an incident occurs. In recognition of the complexity of cyber incidents and 24-hour information technology systems, the SEC Proposed Cyber Rule has proposed a requirement to file a Current Report on Form 8-K about a material cybersecurity incident no later than four business days following determination that the incident is material (rather than the date of discovery of an incident).[8] In acknowledgement of the time-sensitivity of providing notice of a material cyber incident, companies are required

[6] If FCA decides not to defer to the decisions of individual boards of directors about required management reporting about cyber incidents, FCA could add some type of minimum reporting requirements for certain significant events that do not apply to every single cyber incident, e.g., when management determines that a cyber incident potentially presents significant risks to an organization's continuing business operations or safety and soundness.

[7] The term "incident" is not defined in the Proposed Rule and could be interpreted to include a very broad universe of circumstances, including minor incidents that do not involve the loss of sensitive or confidential information and have been resolved.

[8] The SEC Proposed Cyber Rule is not final and is subject to change. The comment period ended on May 9, 2022 and a final rule is expected by Spring 2023.

under the SEC Proposed Cyber Rule to make a determination of materiality of a cyber incident in as prompt a manner as is feasible. Farmer Mac will be subject to reporting material cyber incidents under the final SEC cyber rule amendments when enacted, and we believe that the timing proposed by the SEC Proposed Cyber Rule is appropriate to allow determination of the scope and required actions to address a cyber incident.

Given the time needed to accurately assess the scope of a cyber incident and in light of cyber incidents that occur during non-working hours, we believe that a 36-hour timeline for notification to FCA would be impractical in many cases and impose unnecessary regulatory burden at a time when the focus should be on assessing and resolving a cyber incident. Such a short notification timeframe is also unlikely to result in disclosure of meaningful information about the scope and materiality of a cyber incident. Accordingly, Farmer Mac requests FCA to extend the reporting requirement to four business days after the date of the materiality determination (rather than the date of discovery of the incident), to coincide with the disclosure requirements under the SEC Proposed Cyber Rule.[9]

As noted above, Section 609.930(c)(3)(v) of the Proposed Rule has the potential to require reporting of a wide range of immaterial cyber incidents that do not present material system outages, do not impact reputational risk, or do not lead to a loss of personally identifiable information (PII) or material nonpublic information. Ultimately, the scope and severity of the incident should drive the timing and reporting protocols for the incident. Farmer Mac believes that only those incidents determined to be material should be required notifications to FCA under the Proposed Rule. Regulated institutions should be required to make a materiality determination as soon as reasonably practicable after discovery of a potential cyber incident. The materiality of cyber incidents would be determined after forensic analysis and according to the organization's cyber incident escalation matrix, which would include factors that impact the organization's reputation, operational capacity, financial position, or lead to loss or compromise of a significant amount of sensitive data.

[9] Whatever FCA decides about the appropriate notification timeframe in the final rule, Farmer Mac believes that any notification requirement to FCA should be expressed in terms of business days rather than hours to avoid the possibility of a requirement to notify FCA on a weekend or holiday.

5. Proposed Section 609.930(c)(3)(vi): Notifying customers, employees, and known visitors to an organization's website of an incident.

Farmer Mac believes that aspects of the notification requirement to third parties in proposed Section 609.930(c)(3)(6)[10] are too overbroad and vague to effectively communicate expected behavior consistent with regulatory requirements. Our concerns with this section are similar to some of the concerns expressed above about what types of incidents should be required to be reported to FCA. We believe that the reference to any "incident" involving information provided by third parties without any qualifier related to its materiality or the type of information involved is overbroad in describing situations that should require notifications to third parties. We also believe that "when warranted" does not clarify expectations about when disclosures to third parties should be made if it is attempting to describe situations where disclosures would be expected under FCA's Cyber Risk Management Rules but are not required under other applicable Federal or State law. Farmer Mac suggests that FCA clarify this provision as follows: "Notifying affected third parties of an incident determined by the institution to involve the loss of personally identifiable information or material non-public information if required by applicable State or Federal laws."

6. Proposed Section 609.930(c)(5) Vendor Management and Oversight.

Farmer Mac agrees that vendor diligence, management, and oversight is a critical part of a comprehensive cyber risk management framework. But the proposed requirements in Section 609.930(c)(5)[11] are onerous, not tailored to the risk posed, and would be extremely difficult, if not impossible, for Farmer Mac to impose and implement for all its vendors. This subsection of the Proposed Rule is unnecessarily overbroad and does not effectively define the universe of vendors to which these cyber security rules would apply. As written, the Proposed Rule appears to apply to all vendors regardless of the scale of their relationship with Farmer Mac, their privileged access to Farmer Mac's sensitive information technology systems, or access to PII

[10] An institution's incident response plan must contain procedures for "**[n]otifying** former, current, or potential customers and employees and known visitors to your website **of an incident, when warranted, and in accordance with State and Federal laws**." Proposed Section 609.930(c)(3)(vi) (emphasis added).

[11] Proposed Section 609.930(c)(5)(ii) would require Farmer Mac to require its "vendors" (a term not defined in the Proposed Rule and which could be read to encompass any individual or entity that Farmer Mac conducts business with), by contract, to implement certain measures in compliance with Farmer Mac's cybersecurity plan. Proposed Section 609.930(c)(5)(iii) would require Farmer Mac to actively monitor, audit, and test its vendors' cyber security compliance.

and other material non-public information. We believe that a comprehensive vendor cyber risk management framework should be applied only to those vendors who meet cyber risk exposure metrics such as scale of relationship, access to information technology systems, and access to PII or material nonpublic information.

In its CSF cyber risk profiles, NIST has developed cyber security best practices, risk-based frameworks, and governance guidance that identify organizational cyber risks and create targeted feasible best practices to reduce organizational cyber risk levels. The FFIEC CAT risk-based cybersecurity profiles review the technology services, external threats, technology, and connection types and delivery channels to prioritize internal and external risk-based best practices. These organizational cyber risk best practices developed by cybersecurity professionals and thought leaders create a risk-based framework to assess and manage organizational external cyber risk exposures. Farmer Mac believes that it is through this lens that the vendor management and oversight provisions in the Proposed Rule should be tailored to apply to only those vendors who meet certain organizational cyber risk thresholds, as determined by the organization's cybersecurity plan in the context of its risk appetite.

Farmer Mac is concerned about the potential implications of this section to its vendors in rural America, such as small community banks, regional appraisers, and environmental services companies, who may find compliance with the proposed provisions overly burdensome. For example, these requirements would apply to small rural lenders who are approved loan sellers for Farmer Mac but may have only sold one or two loans to Farmer Mac over time. They would also apply to prospective loan sellers and field servicers that Farmer Mac is seeking to add to its seller/servicer network. In both cases, a requirement that the small lender agree to implement measures consistent with Farmer Mac's cyber risk program and to be audited and tested on those measures by Farmer Mac is likely to be a barrier to doing business with Farmer Mac. Farmer Mac has similar concerns about the application of the proposed vendor management provisions to the independent contractors (most of whom are individuals) that provide important underwriting and appraisal review services as needed on a contract basis. Furthermore, Farmer Mac has hundreds of business counterparties, many of which are non-technical businesses with no access to our technology systems, PII, or material nonpublic information. Examples of these types of vendors include employment recruiting firms, providers of temporary employees, providers of employee training and professional development materials, caterers, office maintenance contractors, event venues, business equipment lessors, providers of audio/visual services, and supply vendors. Farmer Mac believes that its efforts on vendor cybersecurity oversight should be focused where it has maximum impact and not on business relationships where there is little or no cyber risk exposure and that

these types of vendors should not be subject to the proposed requirements in Section 609.930(c)(5) of the Proposed Rule.

Another concern we have with proposed Section 609.930(c)(5)(ii) is that the Proposed Rule provides no guidance for existing vendor relationships and whether all existing vendor contracts would be required to be renegotiated to include retroactive contract provisions for cyber compliance. This would likely prove difficult or in some cases impossible and would require significant allocation of resources. Similarly, proposed Section 609.930(c)(5)(iii) requires institutions to review audits, summaries of test results, or other equivalent evaluations of its vendors, which is likely to pose significant challenges for many vendors who do not currently undertake those activities.

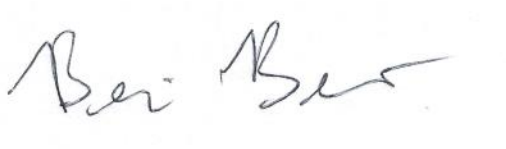
As noted above, Farmer Mac may not be able to require certain small vendors with limited capital and operating budgets to implement specific measures designed to meet the objectives of our cyber risk program. It will also likely be exceedingly difficult to impose cybersecurity compliance requirements under the Proposed Rule on those very large vendors with inflexible contracting processes who already have sophisticated cyber security programs in place. Those types of important vendors that Farmer Mac relies on for much of its information technology infrastructure may not technically align with FCA's guidelines and diligence requirements (e.g., Microsoft, Salesforce, and Bloomberg), including providing access to internal confidential audits, test results, and cyber security evaluations. Indeed, the Proposed Rule could have the unintended consequences of limiting Farmer Mac's ability to contract with smaller rural vendors in furtherance of our mission or very large cyber-mature vendors who likely would not be willing to modify the terms and conditions of their contracts to specifically address the objectives of Farmer Mac's cyber risk program as envisioned in the Proposed Rule.

As discussed, Farmer Mac believes that the vendor management and oversight provisions of the Proposed Rule should be based on a risk-based framework where cyber security programs of critical vendors or vendors that host PII or have access to Farmer Mac's IT systems are reviewed in far greater detail relative to a vendor that does not present significant operational or cybersecurity risks. Farmer Mac requests that Section 609.930(c)(5) of the Proposed Rule be tailored to a risk-based approach in two ways: (1) removing Sections 609.930(c)(5)(ii) and 609.930(c)(5)(iii); and (2) broadening Section 609.930(c)(5)(i) to require each institution to develop and maintain a cyber risk-based vendor management program based on the risk exposure presented by the vendor, and to require enhanced diligence procedures and monitoring of critical vendors or vendors that host PII.

****

Farmer Mac encourages FCA to consider these comments in connection with its preparation of any final regulations. Farmer Mac appreciates FCA's consideration of these comments and would be pleased to discuss these matters further at your request.

Sincerely,



Brian M. Brinch
Senior Vice President – Enterprise Risk Officer